EXHIBIT 1

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WSOU INVESTMENTS, LLC D/B/A BRAZOS LICENSING AND DEVELOPMENT, Plaintiff, v. **CISCO SYSTEMS, INC.,** Defendant.	**Case No. 6:21-CV-00128-ADA** **JURY TRIAL DEMANDED**

PLAINTIFF'S PRELIMINARY INFRINGEMENT CONTENTIONS

In accordance with Section 2 of the Order Governing Proceedings – Patent Case (OGP Version 3.3), Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing and Development ("Brazos" or "Plaintiff"), hereby:

(1) provides its preliminary infringement contentions in the form of charts—attached as Exhibits A, B, C, D, and E—setting forth where in the accused instrumentalities each element of the asserted claims is found;

(2) identifies the priority date (i.e., the earliest date of invention) for each asserted claim; and

(3) provides an accompanying production that includes copies of the certified file histories for each patent-in-suit.

Brazos does not possess documents evidencing conception and reduction to practice for each claimed invention. Brazos reserves the right to further amend or modify its disclosures herein—including to supplement its infringement contentions—based on additional information obtained through discovery or other means concerning Cisco Systems, Inc.'s ("Cisco" or "Defendant") products or services, and/or pending this Court's claim construction order.

I. DISCLOSURE OF PRELIMINARY INFRINGEMENT CONTENTION CHARTS

The patents-in-suit are United States Patent Nos. 8,989,216 ("'216 Patent"), 7,443,859 ("'859 Patent"), 8,191,106 ("'106 Patent"), 8,665,733 ("'733 Patent"), and 9,357,014 ("'014 Patent") (collectively, the "Asserted Patents").

The products accused to infringe the Asserted Patents (the "Accused Products") include, but are not limited to: Cisco ASR 5500, Cisco ASR 5700, Cisco ASR 5000 Small Cell Gateway Series, and Cisco Virtual Packet Core ("'216 Accused Products"); Cisco ASR 5500, Cisco ASR 5700, and Cisco Virtual Packet Core ("'859 Accused Products"); Cisco Cloud Services Router 1000V Series, Cisco 1000 Series Aggregation Services Routers, Cisco ASR 9000 Series Aggregation Services Routers, Cisco 5500 Series Wireless Controllers, Cisco 8500 Series Wireless Controllers, Cisco Virtual Wireless Controller, and Cisco Aironet 1530, 1550, and 1570 Series Outdoor Access Points ("'106 Accused Products"); Cisco 800 Series Industrial Integrated Services Routers, Cisco 800M Integrated Services Router, Cisco 1000 Series Connected Grid Routers, Cisco 2000 Series Connected Grid Routers, Cisco Catalyst 9200 Series Switches, Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, Cisco Catalyst 9500 Series Switches, and Cisco Catalyst 9600 Series Switches ("'733 Accused Products"); and Cisco Ultra Cloud Core and the Cisco Ultra / Virtual Packet Core (VPCSW) ("'014 Accused Products").

The Exhibits set forth representative examples showing where, in the Accused Products, each element of each asserted claim is found. Exhibit A sets forth representative examples showing where in Cisco's Accused Products, each element of each asserted claim of the '216 Patent is found. Exhibit B sets forth representative examples showing where in Cisco's Accused Products, each element of each asserted claim of the '859 Patent is found. Exhibit C sets forth representative examples showing where in Cisco's Accused Products, each element of each asserted claim of the

’106 Patent is found. Exhibit D sets forth representative examples showing where in Cisco’s Accused Products, each element of each asserted claim of the ’733 Patent is found. Exhibit E sets forth representative examples showing where in Cisco’s Accused Products, each element of each asserted claim of the ’014 Patent is found.

As alleged in Plaintiff’s Complaint, ECF No. 1, Defendant also indirectly infringes under 35 U.S.C. § 271(b) & (c) by knowingly encouraging and intending to induce infringement of the Asserted Patents. Specifically, Defendant induces infringement by instructing its customers on how to use and implement the technology claimed in the Asserted Patents. Defendant contributes to infringement of the Asserted Patents by providing the Accused Products within the United States, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the Asserted Patents, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use. Defendant’s infringement is further detailed in Plaintiff’s Complaint, ECF No. 1, which is hereby incorporated by reference in its entirety.

Pursuant to the Order Governing Proceedings – Patent Case (“OGP Version 3.3”), the infringement contentions hereby disclosed by Brazos are preliminary. *See* OGP Version 3.3, § 2, App’x A at row 1 & n. 7. Pursuant to OGP Version 3.3, the deadline to serve final infringement contentions is eight weeks after the *Markman* hearing. *See id*., App’x A at row 17.

These disclosures, including Exhibits A-E, are based on the present state of Brazos’ knowledge, without the benefit of any discovery. Further, Brazos’ investigation is ongoing, and no *Markman* order has been entered in this action. Brazos reserves all rights to supplement, amend, and/or otherwise modify its infringement contentions.

The parties have not exchanged claim terms or proposed claim constructions, Defendant has not served its preliminary invalidity contentions and accompanying production, and the *Markman* hearing date is yet to be determined. Brazos is not required to disclose claim construction positions at this time and does not opt to do so. These disclosures, inclusive of Exhibits A-E, should not be construed as setting forth Brazos' claim construction positions. To the extent Defendant asserts that a particular Brazos claim construction position is implied by these disclosures, including Exhibits A-E, Brazos denies and objects to any such assertion. Brazos reserves all rights to modify its claim construction positions.

II. DISCLOSURE OF THE PRIORITY DATE

The application for the '216 Patent was filed on March 30, 2012. The application does not claim priority to any domestic or international application. Based on information currently available to Brazos, the earliest priority date claimed by Brazos for the '216 Patent is March 30, 2012.

The application for the '859 Patent was filed on December 18, 2001. The application does not claim priority to any domestic or international application. Based on information currently available to Brazos, the earliest priority date claimed by Brazos for the '859 Patent is December 18, 2001.

The application for the '106 Patent was filed on June 7, 2007. The application does not claim priority to any domestic or international application. Based on information currently available to Brazos, the earliest priority date claimed by Brazos for the '106 Patent is June 7, 2007.

The application for the '733 Patent was filed on September 30, 2011. The application does not claim priority to any domestic or international application. Based on information currently

available to Brazos, the earliest priority date claimed by Brazos for the ’733 Patent is September 30, 2011.

The application for the ’014 Patent was filed on April 29, 2014. The application does not claim priority to any domestic or international application. Based on information currently available to Brazos, the earliest priority date claimed by Brazos for the ’014 Patent is April 29, 2014.

These disclosures are based on the present state of Brazos’ knowledge. Further, Brazos’ investigation is ongoing. Brazos reserves all rights to modify the positions taken in these initial disclosures.

III. DISCLOSURES ACCOMPANYING PRODUCTION

These disclosures include an accompanying document production that contains copies of the certified Asserted Patents and the certified file histories for those Patents. The accompanying production is subject to, and does not waive any of, the objections and reservations set forth herein. The Bates number range for the accompanying production is: WSOU-CISCO000001–WSOU-CISCO001846.

Brazos objects to the production of any documents protected by the attorney-client privilege, the work-product doctrine, or any other immunities from discovery.

In producing the accompanying documents, Brazos does not admit or concede the relevancy, materiality, authenticity, or admissibility as evidence of any of these documents. All objections to the use, at trial or otherwise, of any document produced are hereby expressly reserved.

Brazos makes these disclosures without the benefit of discovery. Further, Brazos’ investigation is ongoing. Brazos produces these documents without prejudice to its right to produce

additional documents after considering documents obtained and reviewed throughout discovery and further investigation.

Dated: June 23, 2021

Respectfully submitted,

SUSMAN GODFREY L.L.P.

By: *__/s/ Shawn Blackburn__*

Max L. Tribble, Jr.
Texas Bar No. 2021395
Shawn Blackburn *(pro hac vice)*
Texas Bar No. 24089989
Bryce T. Barcelo *(pro hac vice)*
Texas Bar No. 24092081
1000 Louisiana Street, Suite 5100
Houston, Texas 77002-5096
Telephone: (713) 651-9366
Fax: (713) 654-6666
mtribble@susmangodfrey.com
sblackburn@susmangodfrey.com
bbarcelo@susmangodfrey.com

Kalpana Srinivasan *(pro hac vice)*
California Bar No. 237460
1900 Avenue of the Stars, 14th Floor
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Fax: (310) 789-3150
ksrinivasan@susmangodfrey.com

Danielle M. Nicholson
Washington Bar No. 57873 *(pro hac vice)*
1201 Third Avenue, Suite 3800
Seattle, Washington 98101
Telephone: (206) 516-3880
dnicholson@susmangodfrey.com

Counsel for WSOU Investments, LLC d/b/a Brazos Licensing and Development

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure, I hereby certify that, on June 23, 2021, all counsel of record who have appeared in this case are being served with a copy of the foregoing via email.

/s/ *Danielle M. Nicholson*
Danielle M. Nicholson

EXHIBIT A

EXHIBIT A

U.S. Patent No. 8,989,216 v. Cisco's Mobile Multimedia Gateway Platform

U.S. Patent No. 8,989,216	**Application to Cisco's Mobile Multimedia Gateway Platform**
CLAIM 1	
1[Pre.] A tangible non-transitory storage device readable by a machine, embodying a Diameter protocol command dictionary comprising:	Cisco's Mobile Multimedia Gateway Platform, including, but not limited to, Cisco ASR 5500, Cisco ASR 5700, Cisco ASR 5000 Small Cell Gateway Series, and Cisco Virtual Packet Core, includes a tangible non-transitory storage device readable by a machine, embodying a Diameter protocol command dictionary. For example, the Cisco ASR 5500 includes a tangible storage device, as shown below. · Base 20-slot chassis: 256W · Fabric and storage card (up to 6 per chassis): 100W · System status card (up to 2 per chassis): 10W · Management I/O card (up to 6 per chassis): 900W · Data processing card (up to 8 per chassis): 1000W · Front fan tray (2 per chassis): 60W · Back fan tray (2 per chassis): 840W · Total power (fully loaded): 12,800W · 8 power feeds, capable of carrying 80A each · Operating voltage: -40.5 to -72V *See* Cisco Data Sheet, *Cisco ASR 5500 Multimedia Core Platform*, https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5500/data_sheet_c78-707265.pdf, at 5 (June 2012). Cisco's Mobile Multimedia Gateway Platform also provides various diameter dictionaries, including DPCA, DCCA, CSCF, and Diameter AAA.

Diameter Dictionaries

This section presents information on Diameter dictionary types.

- DPCA
- DCCA
- CSCF
- Diameter AAA

See AAA Interface Administration and Reference, StarOS Release 21.4, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.html#reference_8815aa7a-8a20-4a1e-9dd7-1b6acdcd7f59 (last accessed June 18, 2021).

The exemplary figures below show the configurations of these Diameter dictionaries.

Diameter Dictionaries and Attribute Definitions

This chapter presents information on Diameter dictionary types and attribute definitions.

See Diameter Dictionaries and Attribute Definitions, CISCO, at https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 1 (last accessed June 18, 2021).

DPCA

The Diameter Policy Control Application (DPCA) dictionaries are used by the PDSN, GGSN, HA, IPSG product(s).

To configure the Diameter dictionary for Policy Control Configuration, use the following configuration:

configure
context *<context_name>*
ims-auth-service *<ims_auth_service_name>*
policy-control
diameter dictionary { Standard | dpca-custom1 | dpca-custom10 | dpca-custom11 | dpca-custom12 | dpca-custom13 | dpca-custom14 | dpca-custom15 | dpca-custom16 | dpca-custom17 | dpca-custom18 | dpca-custom19 | dpca-custom2 | dpca-custom20 | dpca-custom21 | dpcacustom22 | dpca-custom23 | dpca-custom24 | dpca-custom25 | dpca-custom26 | dpca-custom27 | dpca-custom28 | dpca-custom29 | dpca-custom3 | dpca-custom30 | dpca-custom4 | dpca-custom5 | dpca-custom6 | dpca-custom7 | dpca-custom8 | dpca-custom9 | dynamic-load | gx-wimax-standard | gxa-3gpp2-standard | gxc-standard | pdsn-ty | r8-gx-standard | std-pdsn-ty | ty-plus | ty-standard }
end

Id. at 12.

DCCA

The Diameter Credit Control Application (DCCA) dictionaries are used by the GGSN and IPSG product(s).

To configure the DCCA dictionary for Active Charging service, use the following configuration:

configure
active-charging service *<acs_service_name>*
credit-control
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-custom16 | dcca-custom17 | dcca-custom18 | dcca-custom19 | dcca-custom2 | dcca-custom20 | dcca-custom21 | dcca-custom22 | dcca-custom23 | dcca-custom24 | dcca-custom25 | dcca-custom26 | dcca-custom27 | dcca-custom28 | dcca-custom29 | dcca-custom3 | dcca-custom30 | dcca-custom4 | dcca-custom5 | dcca-custom6 | dcca-custom7 | dcca-custom8 | dcca-custom9 | dynamic-load | standard }
end

Id. at 13.

	CSCF The Diameter Policy Control dictionaries for Call Session Control Function (CSCF) Diameter Policy External Control Application (DPECA) service are used by the SCM P-CSCF product. In Star OS 8.1 and later releases, to configure the Diameter Policy Control dictionary, use the following configuration: **configure** **context** <*context_name*> **cscf service** <*cscf_service_name*> **proxy-cscf** **diameter policy-control { dictionary { dynamic-load | gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard }** **end** *Id.* **Diameter AAA** The Diameter Authentication, Authorization, and Accounting (AAA) dictionaries are used by the S-CSCF and AIMS product(s). To specify the AAA dictionary to be used when Diameter is being used for accounting, in the AAA Server Group Configuration Mode or in the Context Configuration Mode, use the following command: **diameter accounting dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }** To specify the AAA dictionary to be used when Diameter is being used for authentication, in the AAA Server Group Configuration Mode or in the Context Configuration Mode, use the following command: **diameter authentication dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq }** *Id.* at 14.
1[A] a first definition for a Diameter protocol	Cisco's Mobile Multimedia Gateway Platform includes a first definition for a Diameter protocol command, wherein said Diameter protocol command is defined by a first default definition unless a first context applies

command, wherein said Diameter protocol command is defined by a first default definition unless a first context applies in which case said command is defined by a context-specific definition, and the Diameter protocol command dictionary supports multiple versions of a standard, a second definition for a Diameter protocol attribute value pair (AVP), wherein said Diameter protocol or AVP is defined by a second default definition unless a second context applies in which case said AVP is defined by a second context-specific definition, wherein said Diameter protocol command dictionary

in which case said command is defined by a context specific definition, and the Diameter protocol command dictionary supports multiple versions of a standard, as shown below.

DCCA

The Diameter Credit Control Application (DCCA) dictionaries are used by the GGSN and IPSG product(s).

To configure the DCCA dictionary for Active Charging service, use the following configuration:

```
configure
    active-charging service <acs_service_name>
        credit-control
            diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custo
            end
```

Dictionary	Description
dcca-custom1 ... dcca-custom*n*	Custom-defined dictionaries.
standard	Specifies standard attributes for the Gy interface.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.

Id. at 13.

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }

Specifies the Diameter accounting dictionary.

aaa-custom1 ... aaa-custom10 : Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

<table>
<tr>
<td>interoperates with a Diameter protocol stack to perform functions for processing Diameter messages.</td>
<td>
See AAA Server Group Configuration Mode Commands, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 4 (last accessed June 18, 2021).
Further to this example, Cisco's Mobile Multimedia Gateway Platform includes Diameter protocol command dictionary that supports multiple versions of a standard, for example:
dictionary dictionary
Specifies which dictionary to use. The following table describes the possible values for dictionar
<table>
<tr><th>Dictionary</th><th>Description</th></tr>
<tr><td>customXX</td><td>These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative.
XX is the integer value of the custom dictionary.</td></tr>
<tr><td>standard</td><td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td></tr>
<tr><td>3gpp</td><td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.</td></tr>
<tr><td>3gpp2</td><td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td></tr>
<tr><td>3gpp2-835</td><td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td></tr>
<tr><td>starent-vsa1</td><td>This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA</td></tr>
</table>
Id. at 20.
For example, the Cisco ASR 5500 Series Multimedia Core Platform is a high-capacity platform, specifically designed to satisfy the high performance, subscriber counts, and transaction rates of third-generation (3G) and 4G Long-Term Evolution (LTE) services plus the emergence of small cells. The Cisco ASR 5500 supports an elastic architecture for mobile functions, in which these functions are based on software, not coupled to hardware. The ASR 5500 harvests system resources and applies them across the entire platform to optimize performance and maximize capital efficiency. See Cisco Data Sheet, Cisco ASR 5500 Multimedia Core
</td>
</tr>
</table>

Platform, https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5500/data_sheet_c78-707265.pdf, at 1 (last accessed June 18, 2021).

Cisco ASR 5500 Multimedia Core Platform

As a mobile operator, the mobile broadband network that you built has forever changed the way that your customers work, live, play, and learn, and has become part of the very fabric of their everyday lives. However, mobile operators today face a significant challenge. Data traffic continues to grow exponentially, and regular network modifications are required to keep customers happy. New devices and applications are also drastically changing the way the network behaves. Competition in the mobile market is fierce, as the typical subscriber has multiple options for mobile service. At the same time, revenues are increasingly under pressure. It is an age-old dilemma - how does one reduce cost and increase revenue?

To overcome these challenges, operators must build their core networks with three essential attributes: flexibility, intelligence, and scale. A flexible network is one that can adapt to frequently changing business models, with the ability to make in-network design modifications without huge capital expenditures. An intelligent network is one that recognizes the myriad of different user behavior patterns, and has the tools in place to allow operators to monetize these patterns quickly and transparently. Finally, a scalable network is one that can address the demands of today's mobile network requirements as well as those that will evolve in the future. Data traffic is not just increasing; it is becoming more complex, requiring a scalable and flexible solution across all performance parameters - throughput, transactions, bearers, and sessions.

With all these factors, mobile operators need a mobile packet core solution that they can count on - one that provides efficient evolution to fourth-generation (4G) technology and small cells. Operators must plan for the 'new normal' of the mobile internet - elastic, flexible, virtual. This means being able to harness the right resources (intelligent performance) when you need them - instantaneously. This new normal starts with the intelligent performance of the Cisco® ASR 5500 Multimedia Core Platform (Figure 1). Cisco ASR 5500 sets a new standard for intelligent performance that redefines the economics of the packet core. It is the first mobile platform designed for terabit performance that scales to tens of millions of sessions, and supports the transaction rates required to address the signaling surge.

Figure 1. Cisco ASR 5500 Multimedia Core Platform

Id.

	The storage device in Cisco's Mobile Multimedia Gateway Platform also embodies a Diameter protocol command dictionary comprising a second definition for a Diameter protocol attribute value pair (AVP), wherein said command or AVP is defined by a second default definition unless a second context applies in which case said AVP is defined by a second context-specific definition, wherein said Diameter protocol command dictionary interoperates with a Diameter protocol stack to perform functions for processing Diameter messages, as shown below. **Diameter Attributes** Diameter Attribute Value Pairs (AVPs) carry specific authentication, accounting, authorization, routing and security information as well as configuration details for the request and reply. Some AVPs may be listed more than once. The effect of such an AVP is specific, and is specified in each case by the AVP description. Each AVP of type OctetString must be padded to align on a 32-bit boundary, while other AVP types align naturally. A number of zero-valued bytes are added to the end of the AVP Data field till a word boundary is reached. The length of the padding is not reflected in the AVP Length field. *See Diameter Dictionaries and Attribute Definitions*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 1 (last accessed June 18, 2021).

Vendor-ID	This field is optional. The Vendor-ID field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA assigned "SMI Network Management Private Enterprise Codes" value, encoded in network byte order. Any vendor wishing to implement a vendor-specific Diameter AVP MUST use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications. A vendor ID value of zero (0) corresponds to the IETF adopted AVP values, as managed by the IANA. Since the absence of the vendor ID field implies that the AVP in question is not vendor specific, implementations MUST NOT use the zero (0) vendor ID.

Id. at 4.

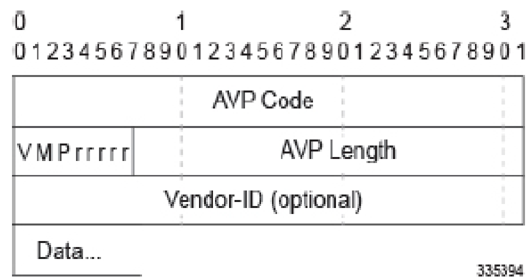


Table 1: AVP Header Details

Field	Description
AVP Code	The AVP Code, combined with the Vendor-ID field, identifies the attribute uniquely. AVP numbers 1 through 255 are reserved for backward compatibility with RADIUS, without setting the Vendor-ID field. AVP numbers 256 and above are used for Diameter, which are allocated by IANA.

Id. at 2.

	(see embedded table below) *Id*. at 12.

Dictionary	Description
Standard	Specifies standard attributes for the Rel 6 Gx interface.
dpca-custom1...dpca-custom*n*	Custom-defined dictionaries.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
gx-wimax-standard	Specifies standard Gx WiMAX Standard attributes.
gxa-3gpp2-standard	Specifies standard Gxa 3GPP2 Standard attributes.
gxc-standard	Specifies Gxc Standard attributes.
pdsn-ty	Specifies the standard attributes for the PDSN Ty interface.
r8-gx-standard	Specifies standard R8 Gx attributes.
std-pdsn-ty	Specifies standard attributes for the Ty interface.
ty-plus	Specifies customer-specific enhanced attributes for the Ty interface.
ty-standard	Specifies standard Ty attributes.

Id. at 12.

CLAIM 2

2[A] The tangible non-transitory storage device of claim 1, wherein said specific context comprises a specific version of a 3rd Generation Partnership Project (3GPP) standard.	Cisco's Mobile Multimedia Gateway Platform includes a tangible non-transitory storage device as described in claim 1, *see supra* 1[Pre.]-1[A], wherein said specific context comprises a specific version of a 3rd Generation Partnership Project (3GPP) standard. For example, the Cisco ASR 5500 includes specific versions of 3GPP standards, as shown below.

GSM/UMTS (CS Domain)	• 3GPP TS 24.008, 48.006, 48.008, 25.413, 29.232, Q.1950, 23.003, 29.002, 23.039, 23.040, 23.401, 23.402, 24.011, 24.080, 24.081, 24.083, 24.084, 24.091, 24.173, 23.009, 49.008

See Cisco Data Sheet, *Cisco ASR 5500 Multimedia Core Platform*, https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5500/data_sheet_c78-707265.pdf, at 5 (last accessed June 18, 2021).

Dictionary	Description
custom*XX*	These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.

See AAA Server Group Configuration Mode Commands, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 20 (last accessed June 19, 2021).

CLAIM 4

4[Pre.] A network node comprising a Diameter protocol command dictionary comprising:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform includes a network node comprising a Diameter protocol command dictionary. *See supra* 1[A].

<table>
<tr>
<td>4[A] a first definition for a Diameter protocol command, wherein said Diameter protocol command is defined by a first default definition unless a first context applies in which case said command is defined by a context-specific definition, and the Diameter protocol command dictionary supports multiple versions of a standard, a second definition for a Diameter protocol attribute value pair (AVP), wherein said command or AVP is defined by a second default definition unless a second context applies in which case said AVP is defined by a second context-specific definition, wherein said</td>
<td>The Diameter protocol command dictionary in Cisco's Mobile Multimedia Gateway Platform comprises a first definition for a Diameter protocol command, wherein said Diameter protocol command is defined by a first default definition unless a first context applies in which case said command is defined by a context-specific definition, and the Diameter protocol command dictionary supports multiple versions of a standard, as shown below. See supra 1[A].

DCCA

The Diameter Credit Control Application (DCCA) dictionaries are used by the GGSN and IPSG product(s).

To configure the DCCA dictionary for Active Charging service, use the following configuration:

configure
active-charging service <acs_service_name>
credit-control
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custo
end

<table>
<tr><th>Dictionary</th><th>Description</th></tr>
<tr><td>dcca-custom1 ... dcca-customn</td><td>Custom-defined dictionaries.</td></tr>
<tr><td>standard</td><td>Specifies standard attributes for the Gy interface.</td></tr>
<tr><td>dynamic load</td><td>Specifies the dynamically loaded Diameter dictionary attributes.</td></tr>
</table>

See Diameter Dictionaries and Attribute Definitions, CISCO, at https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 13 (last accessed June 18, 2021).</td>
</tr>
</table>

Diameter protocol command dictionary interoperates with a Diameter protocol stack to perform functions for processing Diameter messages.	**dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }** Specifies the Diameter accounting dictionary. **aaa-custom1 ... aaa-custom10** : Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used. *See AAA Server Group Configuration Mode Commands*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 4 (last accessed June 18, 2021). Further to this example, Cisco's Mobile Multimedia Gateway Platform includes a Diameter protocol command dictionary that supports multiple versions of a standard, for example:

dictionary *dictionary*

Specifies which dictionary to use. The following table describes the possible values for *dictionar*

Dictionary	Description
custom*XX*	These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA

Id. at 20.

For example, the Cisco ASR 5500 Series Multimedia Core Platform is a high-capacity platform, specifically designed to satisfy the high performance, subscriber counts, and transaction rates of third-generation (3G) and 4G Long-Term Evolution (LTE) services plus the emergence of small cells. The Cisco ASR 5500 supports an elastic architecture for mobile functions, in which these functions are based on software, not coupled to hardware. The ASR 5500 harvests system resources and applies them across the entire platform to optimize performance and maximize capital efficiency. *See* Cisco Data Sheet, *Cisco ASR 5500 Multimedia Core Platform*, https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5500/data_sheet_c78-707265.pdf, at 1 (last accessed June 18, 2021).

Cisco ASR 5500 Multimedia Core Platform

As a mobile operator, the mobile broadband network that you built has forever changed the way that your customers work, live, play, and learn, and has become part of the very fabric of their everyday lives. However, mobile operators today face a significant challenge. Data traffic continues to grow exponentially, and regular network modifications are required to keep customers happy. New devices and applications are also drastically changing the way the network behaves. Competition in the mobile market is fierce, as the typical subscriber has multiple options for mobile service. At the same time, revenues are increasingly under pressure. It is an age-old dilemma - how does one reduce cost and increase revenue?

To overcome these challenges, operators must build their core networks with three essential attributes: flexibility, intelligence, and scale. A flexible network is one that can adapt to frequently changing business models, with the ability to make in-network design modifications without huge capital expenditures. An intelligent network is one that recognizes the myriad of different user behavior patterns, and has the tools in place to allow operators to monetize these patterns quickly and transparently. Finally, a scalable network is one that can address the demands of today's mobile network requirements as well as those that will evolve in the future. Data traffic is not just increasing; it is becoming more complex, requiring a scalable and flexible solution across all performance parameters - throughput, transactions, bearers, and sessions.

With all these factors, mobile operators need a mobile packet core solution that they can count on - one that provides efficient evolution to fourth-generation (4G) technology and small cells. Operators must plan for the 'new normal' of the mobile internet - elastic, flexible, virtual. This means being able to harness the right resources (intelligent performance) when you need them - instantaneously. This new normal starts with the intelligent performance of the Cisco® ASR 5500 Multimedia Core Platform (Figure 1). Cisco ASR 5500 sets a new standard for intelligent performance that redefines the economics of the packet core. It is the first mobile platform designed for terabit performance that scales to tens of millions of sessions, and supports the transaction rates required to address the signaling surge.

Figure 1. Cisco ASR 5500 Multimedia Core Platform

Id.

The Diameter protocol command dictionary in Cisco's Mobile Multimedia Gateway Platform also comprises a second definition for a Diameter protocol attribute value pair (AVP), wherein said command or AVP is defined by a second default definition unless a second context applies in which case said AVP is defined by a

second context-specific definition, wherein said Diameter protocol command dictionary interoperates with a Diameter protocol stack to perform functions for processing Diameter messages.

Diameter Attributes

Diameter Attribute Value Pairs (AVPs) carry specific authentication, accounting, authorization, routing and security information as well as configuration details for the request and reply.

Some AVPs may be listed more than once. The effect of such an AVP is specific, and is specified in each case by the AVP description.

Each AVP of type OctetString must be padded to align on a 32-bit boundary, while other AVP types align naturally. A number of zero-valued bytes are added to the end of the AVP Data field till a word boundary is reached. The length of the padding is not reflected in the AVP Length field.

See Diameter Dictionaries and Attribute Definitions, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 1 (last accessed June 18, 2021).

Vendor-ID	This field is optional. The Vendor-ID field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA assigned "SMI Network Management Private Enterprise Codes" value, encoded in network byte order. Any vendor wishing to implement a vendor-specific Diameter AVP MUST use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications. A vendor ID value of zero (0) corresponds to the IETF adopted AVP values, as managed by the IANA. Since the absence of the vendor ID field implies that the AVP in question is not vendor specific, implementations MUST NOT use the zero (0) vendor ID.

Id. at 4.

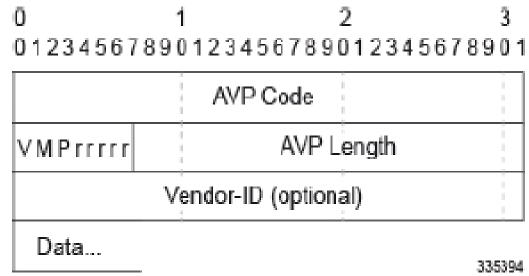


Table 1: AVP Header Details

Field	**Description**
AVP Code	The AVP Code, combined with the Vendor-ID field, identifies the attribute uniquely. AVP numbers 1 through 255 are reserved for backward compatibility with RADIUS, without setting the Vendor-ID field. AVP numbers 256 and above are used for Diameter, which are allocated by IANA.

Id. at 2.

<table>
<tr><td></td><td>

Dictionary	Description
Standard	Specifies standard attributes for the Rel 6 Gx interface.
dpca-custom1...dpca-custom*n*	Custom-defined dictionaries.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
gx-wimax-standard	Specifies standard Gx WiMAX Standard attributes.
gxa-3gpp2-standard	Specifies standard Gxa 3GPP2 Standard attributes.
gxc-standard	Specifies Gxc Standard attributes.
pdsn-ty	Specifies the standard attributes for the PDSN Ty interface.
r8-gx-standard	Specifies standard R8 Gx attributes.
std-pdsn-ty	Specifies standard attributes for the Ty interface.
ty-plus	Specifies customer-specific enhanced attributes for the Ty interface.
ty-standard	Specifies standard Ty attributes.

Id. at 12.</td></tr>
<tr><td colspan="2">CLAIM 5</td></tr>
<tr><td>5[A] The network node of claim 4, wherein said specific context comprises a specific version of a 3rd Generation Partnership Project (3GPP) standard.</td><td>Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 4, see supra 4[Pre.]-4[A], wherein said specific context comprises a specific version of a 3rd Generation Partnership Project (3GPP) standard.

For example, the Cisco ASR 5500 includes specific versions of 3GPP standards, as shown below.

GSM/UMTS (CS Domain)	• 3GPP TS 24.008, 48.006, 48.008, 25.413, 29.232, Q.1950, 23.003, 29.002, 23.039, 23.040, 23.401, 23.402, 24.011, 24.080, 24.081, 24.083, 24.084, 24.091, 24.173, 23.009, 49.008

See Cisco Data Sheet, Cisco ASR 5500 Multimedia Core Platform, https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5500/data_sheet_c78-707265.pdf, at 5 (last accessed June 18, 2021).</td></tr>
</table>

Dictionary	Description
custom*XX*	These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.

See AAA Server Group Configuration Mode Commands, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 20 (last accessed June 19, 2021).

CLAIM 7

7[A] The tangible non-transitory storage device of claim 2, wherein said context can be a major release or a minor release of said 3GPP Standard.	Cisco's Mobile Multimedia Gateway Platform comprises the tangible non-transitory storage device of claim 2, *see supra* 2[A], wherein said context can be a major release or a minor release of said 3GPP Standard. For example, the Diameter Policy Control Application (DPCA) dictionary includes Release 6 and 8 of said 3GPP standard, as shown below.

	<table><tr><th>Dictionary</th><th>Description</th></tr><tr><td>Standard</td><td>Specifies standard attributes for the Rel 6 Gx interface.</td></tr><tr><td>dpca-custom1...dpca-custom*n*</td><td>Custom-defined dictionaries.</td></tr><tr><td>dynamic load</td><td>Specifies the dynamically loaded Diameter dictionary attributes.</td></tr><tr><td>gx-wimax-standard</td><td>Specifies standard Gx WiMAX Standard attributes.</td></tr><tr><td>gxa-3gpp2-standard</td><td>Specifies standard Gxa 3GPP2 Standard attributes.</td></tr><tr><td>gxc-standard</td><td>Specifies Gxc Standard attributes.</td></tr><tr><td>pdsn-ty</td><td>Specifies the standard attributes for the PDSN Ty interface.</td></tr><tr><td>r8-gx-standard</td><td>Specifies standard R8 Gx attributes.</td></tr><tr><td>std-pdsn-ty</td><td>Specifies standard attributes for the Ty interface.</td></tr><tr><td>ty-plus</td><td>Specifies customer-specific enhanced attributes for the Ty interface.</td></tr><tr><td>ty-standard</td><td>Specifies standard Ty attributes.</td></tr></table> *See Diameter Dictionaries and Attribute Definitions*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 12 (last accessed June 19, 2021). By way of another example, the Call Session Control Function (CSCF) Diameter dictionary includes Release 8 of said 3GPP standard, as shown below.

	<table><tr><th>Dictionary</th><th>Description</th></tr><tr><td>dynamic load</td><td>Specifies the dynamically loaded Diameter dictionary attributes.</td></tr><tr><td>gq-custom</td><td>Specifies customized attributes for the 3GPP Gq interface.</td></tr><tr><td>gq-standard</td><td>Specifies standard attributes for the 3GPP Gq interface.</td></tr><tr><td>rq-custom</td><td>Custom-defined dictionary.</td></tr><tr><td>rx-rel8</td><td>Rel. 8 Rx dictionary.</td></tr><tr><td>rx-standard</td><td>Specifies standard attributes for the 3GPP Rx interface.</td></tr><tr><td>tx-standard</td><td>Specifies the standard attributes for the 3GPP2 Tx interface.</td></tr><tr><td>rx-custom01...rx-custom05</td><td>Custom-defined dictionaries.</td></tr></table> *Id*. at 14.
CLAIM 8	
8[A] The tangible non-transitory storage device of claim 7, wherein said minor release of said 3GPP standard may be identified by either a specific version number or release date.	Cisco's Mobile Multimedia Gateway Platform comprises the tangible non-transitory storage device of claim 7, *see supra* 7[A], wherein said minor release of said 3GPP standard may be identified by either a specific version number or release date. For example, the minor release of said 3GPP standard may be identified by a specific version number or release date, as shown below.

	upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 } Specifies to upgrade Diameter accounting dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version. **3gpp-rel10** : Upgrades the dictionary to 3GPP Rel. 10 version. **3gpp-rel9** : Upgrades the dictionary to 3GPP Rel. 9 version. Default: Sets the release version to 3GPP Rel. 8 *See AAA Server Group Configuration Mode Commands*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 6 (last accessed June 19, 2021).
CLAIM 9	
9[A] The network node of claim 5, wherein said context can be a major release or a minor release of said 3GPP standard.	Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 5, *see supra* 5[A], wherein said context can be a major release or a minor release of said 3GPP standard. For example, the Diameter Policy Control Application (DPCA) dictionary includes Release 6 and 8 of said 3GPP standard, as shown below.

Dictionary	Description
Standard	Specifies standard attributes for the Rel 6 Gx interface.
dpca-custom1...dpca-custom*n*	Custom-defined dictionaries.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
gx-wimax-standard	Specifies standard Gx WiMAX Standard attributes.
gxa-3gpp2-standard	Specifies standard Gxa 3GPP2 Standard attributes.
gxc-standard	Specifies Gxc Standard attributes.
pdsn-ty	Specifies the standard attributes for the PDSN Ty interface.
r8-gx-standard	Specifies standard R8 Gx attributes.
std-pdsn-ty	Specifies standard attributes for the Ty interface.
ty-plus	Specifies customer-specific enhanced attributes for the Ty interface.
ty-standard	Specifies standard Ty attributes.

See Diameter Dictionaries and Attribute Definitions, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 12 (last accessed June 19, 2021).

By way of another example, the Call Session Control Function (CSCF) Diameter dictionary includes Release 8 of said 3GPP standard, as shown below.

Dictionary	Description
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
gq-custom	Specifies customized attributes for the 3GPP Gq interface.
gq-standard	Specifies standard attributes for the 3GPP Gq interface.
rq-custom	Custom-defined dictionary.
rx-rel8	Rel. 8 Rx dictionary.
rx-standard	Specifies standard attributes for the 3GPP Rx interface.
tx-standard	Specifies the standard attributes for the 3GPP2 Tx interface.
rx-custom01...rx-custom05	Custom-defined dictionaries.

Id. at 14.

CLAIM 10

10[A] The network node of claim 9, wherein said minor release of said 3GPP standard may be identified by either a specific version number or release date.	Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 9, *see supra* 9[A], wherein said minor release of said 3GPP standard may be identified by either a specific version number or release date. For example, the minor release of said 3GPP standard may be identified by a specific version number or release date, as shown below.

	upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 } Specifies to upgrade Diameter accounting dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version. **3gpp-rel10** : Upgrades the dictionary to 3GPP Rel. 10 version. **3gpp-rel9** : Upgrades the dictionary to 3GPP Rel. 9 version. Default: Sets the release version to 3GPP Rel. 8 *See AAA Server Group Configuration Mode Commands*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 6 (last accessed June 19, 2021).
CLAIM 11	
11[Pre.] A network node comprising a Diameter protocol command dictionary comprising:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform consists of a network node comprising a Diameter protocol command dictionary. *See supra* 1[A], 4[Pre.].
11[A] a definition for a Diameter protocol command, wherein the Diameter protocol command comprises a command default definition and a command first context specific definition; and a definition for a Diameter protocol	Cisco's Mobile Multimedia Gateway Platform consists of a network node comprising a Diameter protocol command dictionary comprising a definition for a Diameter protocol command, wherein the Diameter protocol command comprises a command default definition and a command first context specific definition.

<table>
<tr>
<td>attribute value pair (AVP), wherein the Diameter protocol AVP comprises an AVP default definition and an AVP first context specific definition and the Diameter protocol dictionary supports multiple versions of a standard, where said Diameter protocol command dictionary interoperates with a Diameter protocol to perform functions for processing Diameter messages.</td>
<td>

DCCA

The Diameter Credit Control Application (DCCA) dictionaries are used by the GGSN and IPSG product(s).

To configure the DCCA dictionary for Active Charging service, use the following configuration:

<pre>
configure
    active-charging service <acs_service_name>
        credit-control
            diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custo
            end
</pre>

<table>
<tr><th>Dictionary</th><th>Description</th></tr>
<tr><td>dcca-custom1 ... dcca-customn</td><td>Custom-defined dictionaries.</td></tr>
<tr><td>standard</td><td>Specifies standard attributes for the Gy interface.</td></tr>
<tr><td>dynamic load</td><td>Specifies the dynamically loaded Diameter dictionary attributes.</td></tr>
</table>

See Diameter Dictionaries and Attribute Definitions, CISCO, at https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 13 (last accessed June 18, 2021).

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }

Specifies the Diameter accounting dictionary.

aaa-custom1 ... aaa-custom10 : Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

</td>
</tr>
</table>

See AAA Server Group Configuration Mode Commands, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 4 (last accessed June 18, 2021).

The Diameter protocol command dictionary in Cisco's Mobile Multimedia Gateway Platform also comprises a definition for a Diameter protocol attribute value pair (AVP), wherein the Diameter protocol AVP comprises an AVP default definition and an AVP first context specific definition and the Diameter protocol dictionary supports multiple versions of a standard, where said Diameter protocol command dictionary interoperates with a Diameter protocol to perform functions for processing Diameter messages.

Diameter Attributes

Diameter Attribute Value Pairs (AVPs) carry specific authentication, accounting, authorization, routing and security information as well as configuration details for the request and reply.

Some AVPs may be listed more than once. The effect of such an AVP is specific, and is specified in each case by the AVP description.

Each AVP of type OctetString must be padded to align on a 32-bit boundary, while other AVP types align naturally. A number of zero-valued bytes are added to the end of the AVP Data field till a word boundary is reached. The length of the padding is not reflected in the AVP Length field.

See Diameter Dictionaries and Attribute Definitions, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 1 (last accessed June 18, 2021).

	Vendor-ID: This field is optional. The Vendor-ID field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA assigned "SMI Network Management Private Enterprise Codes" value, encoded in network byte order. Any vendor wishing to implement a vendor-specific Diameter AVP MUST use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications. A vendor ID value of zero (0) corresponds to the IETF adopted AVP values, as managed by the IANA. Since the absence of the vendor ID field implies that the AVP in question is not vendor specific, implementations MUST NOT use the zero (0) vendor ID. *Id*. at 4.

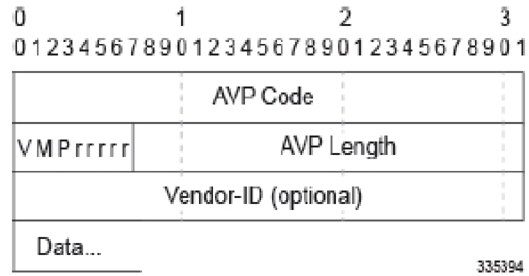


Table 1: AVP Header Details

Field	Description
AVP Code	The AVP Code, combined with the Vendor-ID field, identifies the attribute uniquely. AVP numbers 1 through 255 are reserved for backward compatibility with RADIUS, without setting the Vendor-ID field. AVP numbers 256 and above are used for Diameter, which are allocated by IANA.

Id. at 2.

Dictionary	Description
Standard	Specifies standard attributes for the Rel 6 Gx interface.
dpca-custom1...dpca-custom*n*	Custom-defined dictionaries.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
gx-wimax-standard	Specifies standard Gx WiMAX Standard attributes.
gxa-3gpp2-standard	Specifies standard Gxa 3GPP2 Standard attributes.
gxc-standard	Specifies Gxc Standard attributes.
pdsn-ty	Specifies the standard attributes for the PDSN Ty interface.
r8-gx-standard	Specifies standard R8 Gx attributes.
std-pdsn-ty	Specifies standard attributes for the Ty interface.
ty-plus	Specifies customer-specific enhanced attributes for the Ty interface.
ty-standard	Specifies standard Ty attributes.

Id. at 12.

Further, the Diameter protocol command dictionary supports multiple versions of a standard, for example:

dictionary *dictionary*

Specifies which dictionary to use. The following table describes the possible values for *dictionar*

Dictionary	Description
custom*XX*	These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA

See AAA Server Group Configuration Mode Commands, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 20 (last accessed June 18, 2021).

CLAIM 12

12[A] The network node of claim 11, wherein the Diameter protocol command further comprises a command second context specific definition.	Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 11, *see supra* 11[Pre.]-11[A], wherein the Diameter protocol command further comprises a command second context specific definition. For example, Cisco's Mobile Multimedia Gateway Platform includes multiple context specific definitions, as shown below.

	DCCA
	
	The Diameter Credit Control Application (DCCA) dictionaries are used by the GGSN and IPSG product(s).
	
	To configure the DCCA dictionary for Active Charging service, use the following configuration:
	
	`configure`
	`    active-charging service <acs_service_name>`
	`        credit-control`
	`            diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custo`
	`            end`
	
	Dictionary / **Description**:
	dcca-custom1 ... dcca-custom*n* — Custom-defined dictionaries.
	standard — Specifies standard attributes for the Gy interface.
	dynamic load — Specifies the dynamically loaded Diameter dictionary attributes.
	
	See Diameter Dictionaries and Attribute Definitions, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 12 (last accessed June 18, 2021).

	dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus } Specifies the Diameter accounting dictionary. **aaa-custom1 ... aaa-custom10** : Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used. *See AAA Server Group Configuration Mode Commands*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 4(last accessed June 18, 2021).
CLAIM 13	
13[A] The network node of claim 11, wherein the Diameter protocol AVP further comprises AVP second context specific definition.	Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 11, *see supra* 11[Pre.]-11[A], wherein the Diameter protocol AVP further comprises AVP second context specific definition. For example, the Diameter protocol AVP in Cisco's Mobile Multimedia Gateway Platform includes multiple AVP context specific definitions, as shown below.

	<table><tr><td>Vendor-ID</td><td>This field is optional. The Vendor-ID field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA assigned "SMI Network Management Private Enterprise Codes" value, encoded in network byte order. Any vendor wishing to implement a vendor-specific Diameter AVP MUST use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications. A vendor ID value of zero (0) corresponds to the IETF adopted AVP values, as managed by the IANA. Since the absence of the vendor ID field implies that the AVP in question is not vendor specific, implementations MUST NOT use the zero (0) vendor ID.</td></tr></table> *See Diameter Dictionaries and Attribute Definitions*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 4 (last accessed June 18, 2021).

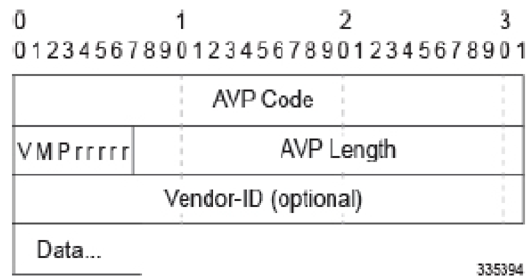


Table 1: AVP Header Details

Field	Description
AVP Code	The AVP Code, combined with the Vendor-ID field, identifies the attribute uniquely. AVP numbers 1 through 255 are reserved for backward compatibility with RADIUS, without setting the Vendor-ID field. AVP numbers 256 and above are used for Diameter, which are allocated by IANA.

See Diameter Dictionaries and Attribute Definitions, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-4_N5-7/AAA/21-4-AAA-Reference/21-AAA-Reference_chapter_01101.pdf, at 2 (last accessed June 18, 2021).

CLAIM 14

14[A] The network node of claim 11, wherein the command first context specific definition and the AVP first context	Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 11, *see supra* 11[Pre.]-11[A], wherein the command first context specific definition and the AVP first context specific definition may be identified by either a Diameter version number or release date, as shown below.

specific definition may be identified by either a Diameter version number or release date.	**upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 }** Specifies to upgrade Diameter accounting dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version. **3gpp-rel10** : Upgrades the dictionary to 3GPP Rel. 10 version. **3gpp-rel9** : Upgrades the dictionary to 3GPP Rel. 9 version. Default: Sets the release version to 3GPP Rel. 8 *See AAA Server Group Configuration Mode Commands*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-10_6-4/Mode_A-B-CLI-Reference/21-10-A-B_CLI-Reference/21-10-A-B_CLI-Reference_chapter_011.pdf, at 6 (last accessed June 19, 2021).
CLAIM 15	
15[A] The tangible non-transitory storage device of claim 1, wherein said Diameter protocol command dictionary is formatted in an Extensible Markup Language (XML) file.	Cisco's Mobile Multimedia Gateway Platform comprises the tangible non-transitory storage device of claim 1, *see supra* 1[Pre.]-1[A], wherein said Diameter protocol command dictionary is formatted in an Extensible Markup Language (XML) file. As shown in the non-limiting example below, the Diameter protocol command dictionary is formatted in an Extensible Markup Language (XML) file published by Cisco.

	2.5. Command Dictionary File TOC The commands that can be parsed by the local Diameter client library or server are defined in a command dictionary file containing the command definitions including AVPs. The location and name of the command dictionary file is platform-specific. This file is read and parsed to drive creation of a command dictionary which is used by the library to parse commands. The syntax for the command dictionary file is in XML and a DTD describing it is available in **[XML]**. XML was selected as the definition language because support for XML parsing is available as an extension to the standard Java APIs and as a wide variety of public-domain C libraries, simplifying implementation. Both APIs also support programmatic definition of commands, AVPs, and extensions so programs can add commands not in the dictionary for purposes of experimentation and implementing the library. *See The Diameter API*, CISCO, https://tools.ietf.org/id/draft-ietf-dime-diameter-api-08.html#anchor8 (last accessed June 19, 2021).
CLAIM 16	
16[A] The network node of claim 4, wherein said Diameter protocol command dictionary is formatted in an Extensible Markup Language (XML) file.	Cisco's Mobile Multimedia Gateway Platform comprises the network node of claim 4, *see supra* 4[Pre.]-4[a], wherein said Diameter protocol command dictionary is formatted in an Extensible Markup Language (XML) file. As shown in the non-limiting example below, the Diameter protocol command dictionary is formatted in an Extensible Markup Language (XML) file published by Cisco.

	2.5. Command Dictionary File TOC The commands that can be parsed by the local Diameter client library or server are defined in a command dictionary file containing the command definitions including AVPs. The location and name of the command dictionary file is platform-specific. This file is read and parsed to drive creation of a command dictionary which is used by the library to parse commands. The syntax for the command dictionary file is in XML and a DTD describing it is available in **[XML]**. XML was selected as the definition language because support for XML parsing is available as an extension to the standard Java APIs and as a wide variety of public-domain C libraries, simplifying implementation. Both APIs also support programmatic definition of commands, AVPs, and extensions so programs can add commands not in the dictionary for purposes of experimentation and implementing the library. *See The Diameter API*, CISCO, https://tools.ietf.org/id/draft-ietf-dime-diameter-api-08.html#anchor8 (last accessed June 19, 2021).

EXHIBIT B

EXHIBIT B

U.S. Patent No. 7,443,859 v. Cisco's Mobile Multimedia Gateway Platform

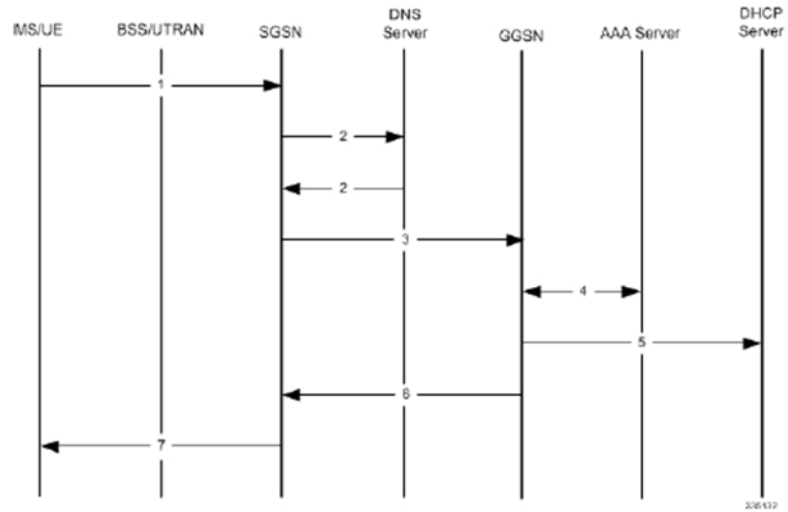
U.S. Patent No. 7,443,859	Application to Cisco's Mobile Multimedia Gateway Platform
CLAIM 1	
1[Pre.] A method comprising:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform, including, but not limited to, Cisco ASR 5500, Cisco ASR 5700, and Cisco Virtual Packet Core, practices a method comprising the elements set forth below. StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to Cisco's Mobile Multimedia Gateway Platform. For example, "StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to the wireless carriers. Functioning as an SGSN, the system readily handles wireless data services within 2.5G General Packet RadioService (GPRS) and 3G Universal Mobile TelecommunicationsSystem (UMTS) data networks. The SGSN also can serve as an interface between GPRS and/or UMTS networks and the 4G Evolved Packet Core (EPC) network." *SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 5 (Aug. 29, 2019) (last accessed June 20, 2021).
1[A] receiving an Activate Packet Data Protocol (PDP) Context Request message at a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network from a	Cisco's Mobile Multimedia Gateway Platform practices a method of receiving an Activate Packet Data Protocol (PDP) Context Request message at a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network from a mobile station of the network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station. For example, as shown below in Step 1, the SGSN receives a PDP Activation Request message from a mobile station (MS) containing an APN field.

mobile station of the network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station; and

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

The APN Restriction value determines the type of application data the subscriber can send. For example, the "APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum APN Restriction of the UE ["User Equipment"] to the GGSN/P-GW in a Create PDP Context Request/Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/Create Session Request." *Id*. at 183.

The APN Restriction values explicitly indicate the request for a private or public network address to be assigned to the mobile station. For example, when the "APN Restriction Value allowed to be established" is "1" then the "Private" APN for Corporate is assigned in the exemplary manner shown below.

Table 13: APN restriction values

Maximum APN Restriction Value	**Type of APN**	**Application Example**	**APN Restriction Value allowed to be established**
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (for example MMS subscribers)	1
4	Private-2	Corporate (for example non-MMS subscribers)	None

Id. at 184.

"Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured." *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 104 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool:

Step 1 Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.

Step 2 Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.

Step 3 Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Id. at 105.

<table>
<tr><td></td><td>

IPv4 Pool Creation

Use the following example to create the IPv4 address pool:

```
configure
    context <dest_ctxt_name>
      ip pool <pool_name> <ip_address/mask> [{private| public}[priority]] | static]
      end
```

Id. at 106.</td></tr>
<tr><td>**1[B]** sending an Activate PDP Context Accept message to the mobile station containing information assigning one of a private network address and a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.</td><td>Cisco's Mobile Multimedia Gateway Platform practices a method of sending an Activate PDP Context Accept message to the mobile station containing information assigning one of a private network address and a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.

For example, as shown below in Step 7, the SGSN sends the Activate PDP Context Accept message to the mobile station (MS) along with the IP Address.

<table><tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address.

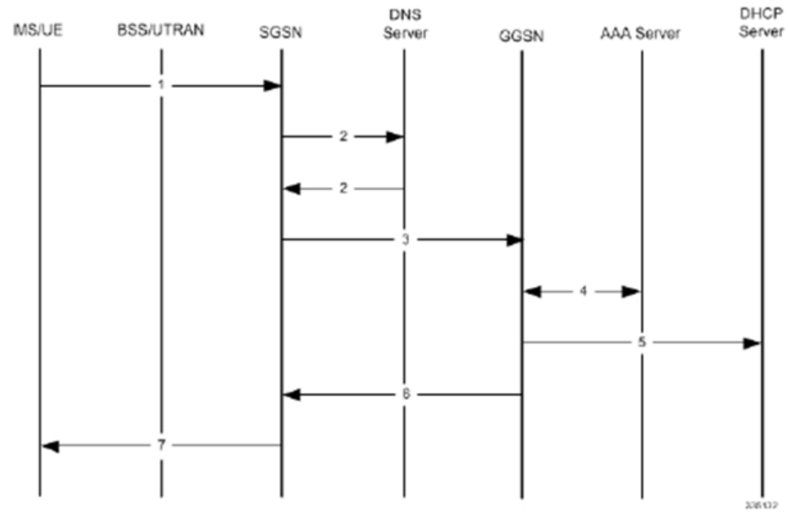
Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions.

A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr></table>
See SGSN Administration Guide, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).</td></tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

The GGSN already has an APN Restriction value for each APN request by UE/MS. The GGSN checks whether the APN Restriction value received in the Create PDP Context Request from the SGSN and the APN Restriction value of the APN to which access is requested are the same. If the values are the same, the GGSN creates the PDP context and sends a create response message back to the SGSN containing the IP address assigned to the UE/MS. The SGSN then sends an Activate PDP Context Accept message to the UE/MS.

	For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id*. at 184.
CLAIM 2	
2[A] The method according to claim 1, further comprising: sending a Create PDP Context Request message from the SGSN to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of the network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 1, *see supra* 1[Pre.]-1[B], further comprising sending a Create PDP Context Request message from the SGSN to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of the network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network address for the mobile station. For example, as shown in Step 3 below, to resolve the received APN in the PDP activation request message, the SGSN sends a Create PDP Context Request to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. The SGSN sends an APN Restriction value (Maximum APN Restriction) in the Create PDP Context Request for establishing a PDP context. 3 | The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context. *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

address for the mobile station; and	

SGSN and Dual Access SGSN Deployments

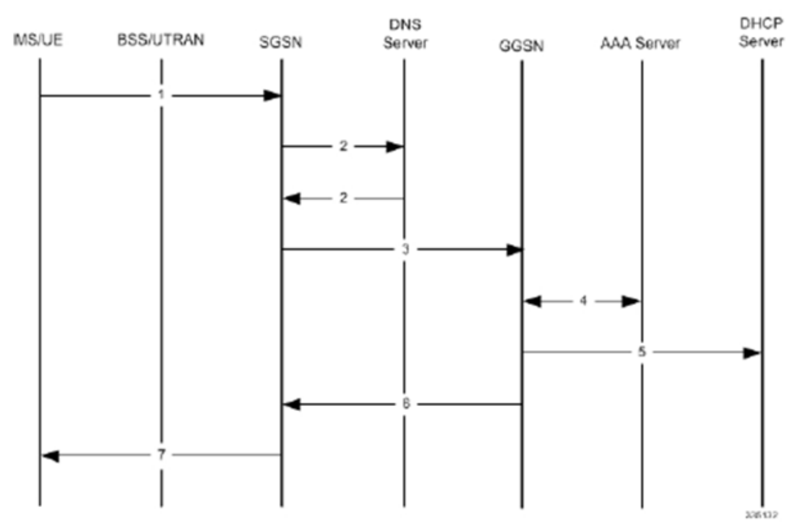
SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on *System Configuration Options*, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services.

Id. at 5.

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

<table>
<tr>
<td></td>
<td>The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, “[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be “0” in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68).” Id. at 184.</td>
</tr>
<tr>
<td>2[B] receiving a Create PDP Context Response message from the GGSN containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 1, see supra 1[Pre.]-1[B], further comprising receiving a Create PDP Context Response message from the GGSN containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.

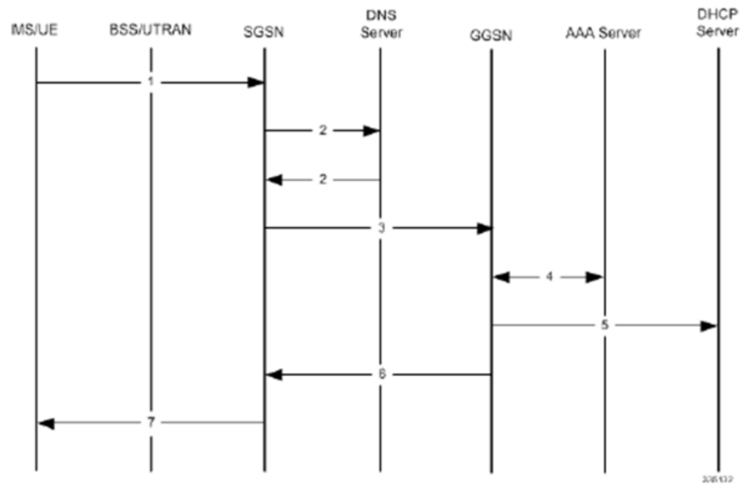
For example, as shown below in Step 6, once an IP address (public or private depending on the APN request) is chosen, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address assigned to the mobile station.

<table><tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr></table>
Id. at 81.</td>
</tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

CLAIM 3	
3[A] The method according to claim 2, further comprising:	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 2, *see supra* 2[A]-2[B], and further comprises receiving the Create PDP Context Request message from the SGSN at the GGSN. For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.

<table>
<tr>
<td>receiving the Create PDP Context Request message from the SGSN at the GGSN;</td>
<td>

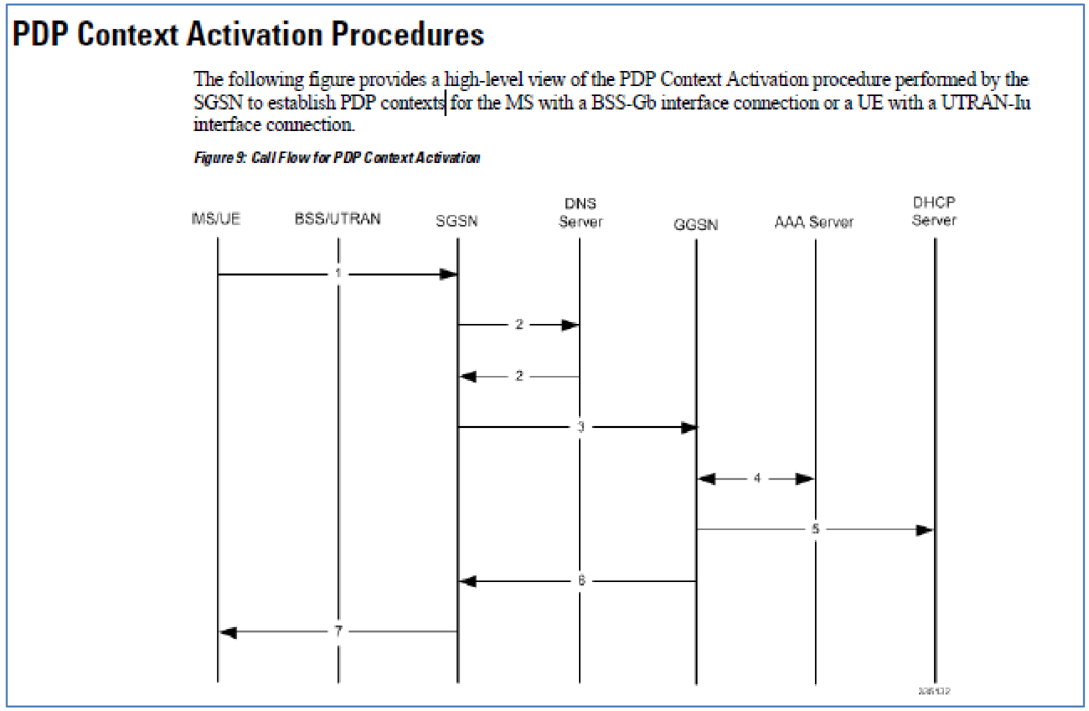
3	The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.

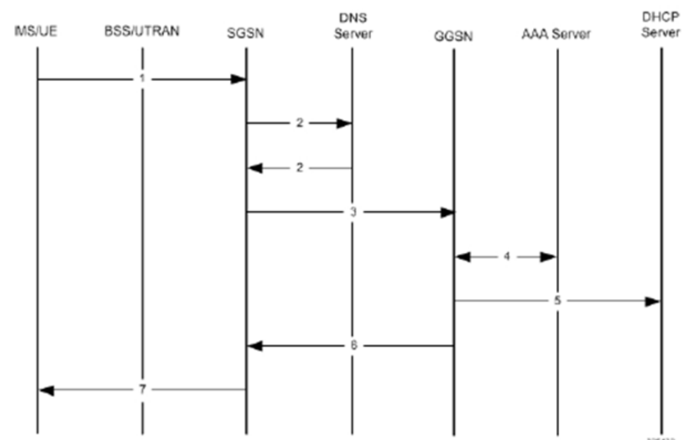
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).
</td>
</tr>
<tr>
<td>3[B] assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message and</td>
<td>

Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 2, *see supra* 2[B], and further comprises assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below, the mobile station is assigned an IP address (public or private) based on the information contained in the APN field of the Create PDP Context Request message.

Step	**Description**
5	If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.
6	The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.
7	The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data.
</td>
</tr>
</table>

	See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).  **PDP Context Activation Procedures** The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection. *Figure 9: Call Flow for PDP Context Activation* *Id*. at 80.
3[C] sending the Create PDP Context Response message from the GGSN to the SGSN containing the information	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 2, *see supra* 2[A]-2[B], and further comprises sending the Create PDP Context Response message from the GGSN to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message. For example, as shown below in Step 6, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address (public or private depending on the APN request) assigned to the mobile station.

assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.	6 — The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE. *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021). **PDP Context Activation Procedures** The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection. *Figure 9: Call Flow for PDP Context Activation*  The following table provides detailed explanations for each step indicated in the figure above. *Table 3: PDP Context Activation Procedure* **Step** — **Description** 1 — The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN). *Id*. at 80.

CLAIM 4	
4[A] The method according to claim 1, further comprising: sending a Create PDP Context Request message from the SGSN to a Border Gateway (BG) of the network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network address for the mobile station; and	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 1, *see supra* 1[Pre.]-1[B], and further comprises sending a Create PDP Context Request message from the SGSN to a Border Gateway (BG) of the network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network address for the mobile station, *see supra* 2[A]-2[B]. For example, StarOS includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, the SGSN sends a Create PDP Context Request message to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) or to a Border Gateway (Packet Gateway: P-GW). *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021). Further to this example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id.* at 184.
4[B] receiving a Create PDP Context Response message at the SGSN from the BG containing information assigning either a private network address or a public	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 1, *see supra* 1[Pre.]-1[B], and further comprises receiving a Create PDP Context Response message at the SGSN from the BG containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message. For example, StarOS includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, the SGSN receives a Create PDP Context Response message from a Gateway General Packet Radio System (GPRS) Support Node (GGSN) or a Border Gateway (Packet Gateway: P-GW). *See SGSN Administration Guide, StarOS Release 21.15*, CISCO,

<table>
<tr><td>network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.</td><td>https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).</td></tr>
<tr><td colspan="2">CLAIM 5</td></tr>
<tr><td>5[A] The method according to claim 4, further comprising: receiving the Create PDP Context Request message at the BG;</td><td>Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 4, see supra 4[A]-4[B], and further comprises, on information and belief, receiving the Create PDP Context Request message at the BG.

For example, StarOS includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, the Border Gateway (Packet Gateway: PW) receives the Create PDP Context Request message. See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).

For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.

<table><tr><td>3</td><td>The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.</td></tr></table>
See id. at 80.</td></tr>
</table>

<table>
<tr>
<td>5[B] assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message; and</td>
<td>
Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 4, see supra 4[A]-4[B], and further comprises assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.
For example, as shown below, the mobile station is assigned an IP address (public or private) based on the information contained in the APN field of the Create PDP Context Request message.
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5</td><td>If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.</td></tr>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
<tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address.

Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions.

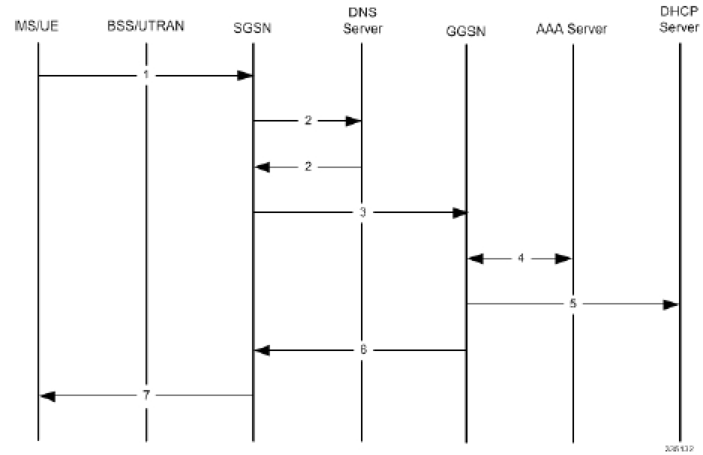
A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr>
</table>
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



Id. at 80.
</td>
</tr>
<tr>
<td>

5[C] sending the Create PDP Context Response message to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the
</td>
<td>

Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 4, *see supra* 4[A]-4[B], and further comprises sending the Create PDP Context Response message to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below in Step 6, the SGSN is sent a Create PDP Context Response message containing the IP address (public or private depending on the APN request) assigned to the mobile station.

<table>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
</table>

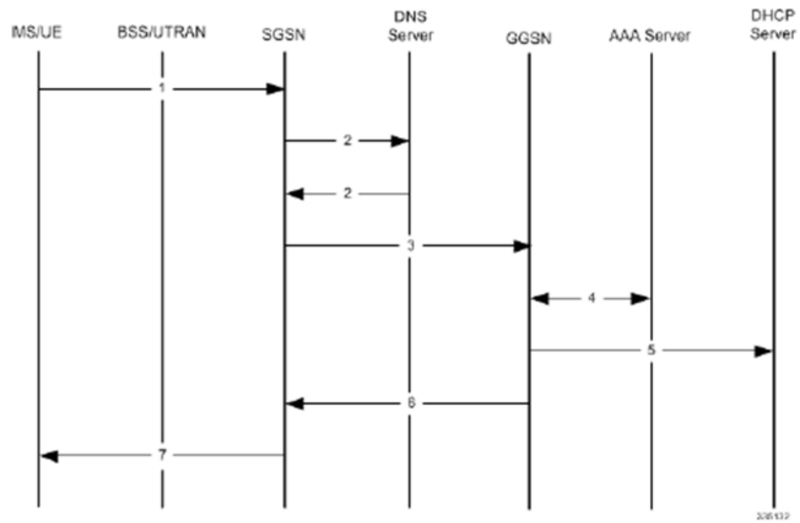
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).
</td>
</tr>
</table>

<table>
<tr>
<td>APN field of the Create PDP Context Request message.</td>
<td>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.
</td>
</tr>
</table>

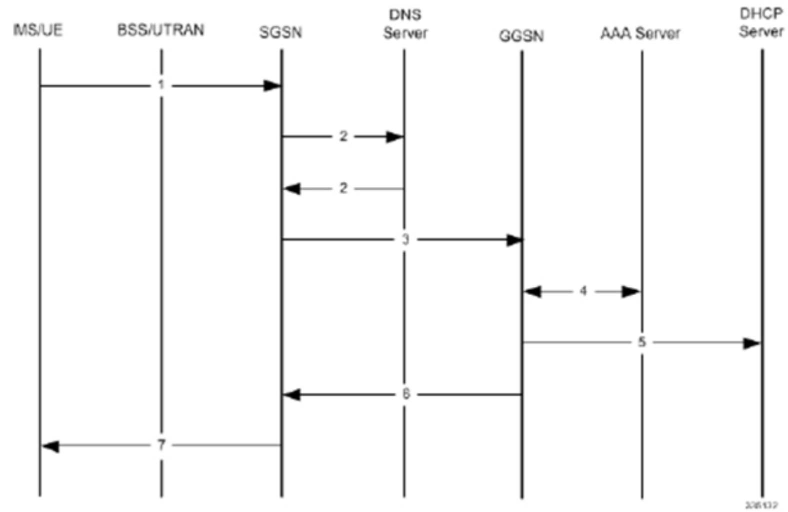
CLAIM 6	
6[A] The method according to claim 5, further comprising: sending the Create PDP Context Request message from the SGSN to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of the network;	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 5, *see supra* 5[A]-5[C], and further comprises sending the Create PDP Context Request message from the SGSN to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of the network. For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request message to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. 3 — The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context. *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

<table>
<tr>
<td></td>
<td>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

</td>
</tr>
<tr>
<td>

6[B] sending the Create PDP Context Request message from the GGSN to the BG;

</td>
<td>

Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 5, *see supra* 5[A]-5[C], and further comprises, on information and belief, sending the Create PDP Context Request message from the GGSN to the Border Gateway (Packet Gateway: P-GW). Cisco's Mobile Multimedia Gateway Platform includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. *Id.* at 6.

</td>
</tr>
</table>

<table>
<tr>
<td>6[C] receiving the Create PDP Context Response message at the GGSN from the BG; and</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 5, see supra 5[A]-5[C], and further comprises, on information and belief, receiving the Create PDP Context Response message at the GGSN from the Border Gateway (Packet Gateway: P-GW). Cisco’s Mobile Multimedia Gateway Platform includes both “Standalone gateway GPRS support node (GGSN)” and “Co-located P-GW/GGSN” deployments and interfaces. Id. at 6.</td>
</tr>
<tr>
<td>6[D] receiving the Create PDP Context Response message at the SGSN from the GGSN.</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 5, see supra 5[A]-5[C], and further comprises receiving the Create PDP Context Response message at the SGSN from the GGSN.

For example, as shown below in Step 6, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address assigned to the mobile station.

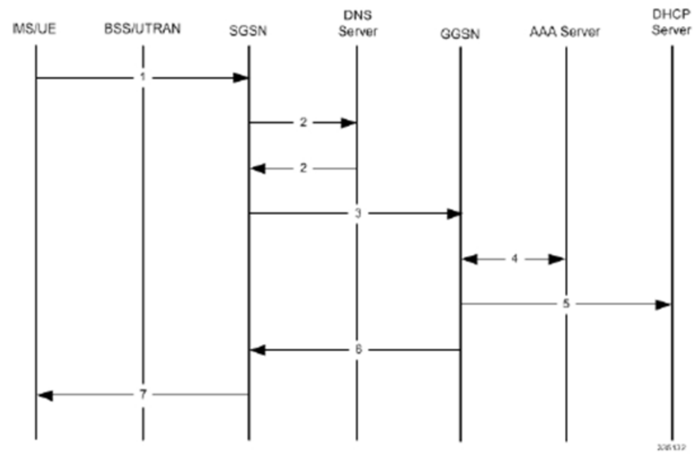
<table>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
</table>

Id. at 81.</td>
</tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

CLAIM 7

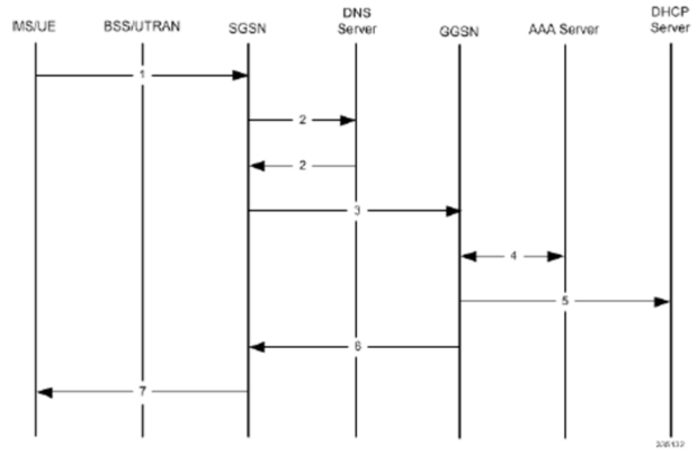
7[A] The method according to claim 1, further comprising receiving at the mobile station the Activate PDP Context Accept	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 1, *see supra* 1[Pre.]-1[B], and further comprises receiving at the mobile station the Activate PDP Context Accept message containing the information relating to an assignment of either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.

<table>
<tr>
<td>message containing the information relating to an assignment of either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.</td>
<td>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>

See SGSN Administration Guide, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

For example, as shown below, the SGSN sends the Activate PDP Context Accept message and IP address to the mobile station (MS).

</td>
</tr>
</table>

	<table><tr><th>Step</th><th>Description</th></tr><tr><td>5</td><td>If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.</td></tr><tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr><tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr></table> *Id*. at 81. The GGSN already has an APN Restriction value for each APN request by UE/MS. The GGSN checks whether the APN Restriction value received in the Create PDP Context Request from the SGSN and the APN Restriction value of the APN to which access is requested are the same. If the values are the same, the GGSN creates the PDP context and sends a create response message back to the SGSN containing the IP address assigned to the UE/MS. The SGSN then sends an Activate PDP Context Accept message to the UE/MS. For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id*. at 184.

<table>
<tr><th colspan="2">CLAIM 8</th></tr>
<tr>
<td>8[A] The method according to claim 1, wherein in the receiving and sending, the information comprises one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station.</td>
<td>
Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 1, see supra 1[Pre.]-1[B], wherein in the receiving and sending, the information comprises one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station.
For example, the APN Restriction value determines the type of application data the subscriber can send. The “APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum APN Restriction of the UE to the GGSN/P-GW in a Create PDP Context Request/Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/Create Session Request.” Id. at 183.
The APN Restriction values explicitly indicate the request for a private or public network address to be assigned to the mobile station. For example, when the “APN Restriction Value allowed to be established” is “1,” then the “Private” APN for Corporate is assigned in the exemplary manner shown below.
Table 13: APN restriction values
<table>
<tr><th>Maximum APN Restriction Value</th><th>Type of APN</th><th>Application Example</th><th>APN Restriction Value allowed to be established</th></tr>
<tr><td>0</td><td colspan="2">No Existing Contexts or Restriction</td><td>All</td></tr>
<tr><td>1</td><td>Public-1</td><td>WAP or MMS</td><td>1, 2, 3</td></tr>
<tr><td>2</td><td>Public-2</td><td>Internet or PSPDN</td><td>1, 2</td></tr>
<tr><td>3</td><td>Private-1</td><td>Corporate (for example MMS subscribers)</td><td>1</td></tr>
<tr><td>4</td><td>Private-2</td><td>Corporate (for example non-MMS subscribers)</td><td>None</td></tr>
</table>
Id. at 184.
“Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured.” GGSN
</td>
</tr>
</table>

	Administration Guide, StarOS Release 21.3, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 104 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool: **Step 1** Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section. **Step 2** Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section. **Step 3** Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section. **Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter. *Id*. at 105. **IPv4 Pool Creation** Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name> <ip_address/mask>* **[{private| public}[priority]] | static]** **end** *Id*. at 106.
CLAIM 9	
9[Pre.] A method comprising:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform practices a method comprising the following elements, as illustrated below.
9[A] receiving a Create Packet Data Protocol (PDP) Context Request message from a Serving General Packet Radio	Cisco's Mobile Multimedia Gateway Platform practices a method that comprises receiving a Create Packet Data Protocol (PDP) Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN) at a Gateway General Packet Radio System (GPRS) Support Node (GGSN), the Create PDP Context Request Message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of the network.

<table>
<tr>
<td>System (GPRS) Support Node (SGSN) at a Gateway General Packet Radio System (GPRS) Support Node (GGSN), the Create PDP Context Request Message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of the network;</td>
<td>For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.

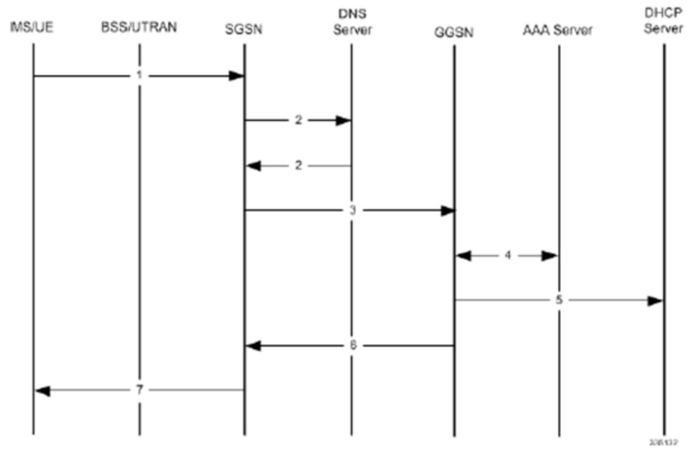
<table><tr><td>3</td><td>The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.</td></tr></table>

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).</td>
</tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

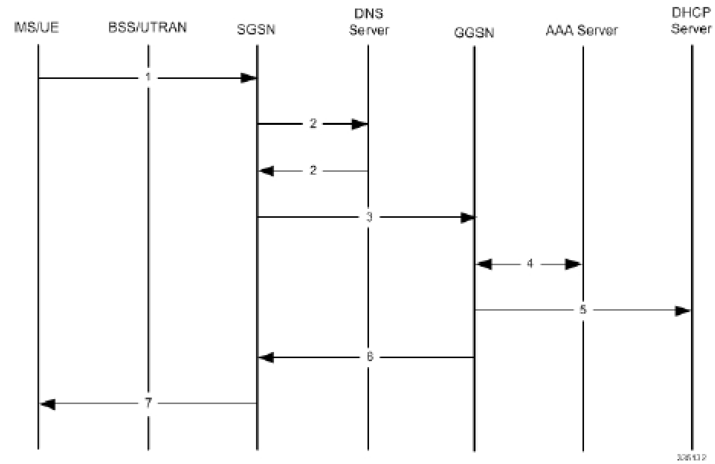
Id. at 80.

The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id.* at 184.

9[B] assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message; and	Cisco's Mobile Multimedia Gateway Platform practices a method that comprises assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message. For example, as shown below, the mobile station is assigned an IP address (public or private) based on the information contained in the APN field of the Create PDP Context Request message. **Step** / **Description** 5 — If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP. 6 — The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE. 7 — The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data. *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).

Embedded table:

Step	Description
5	If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.
6	The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.
7	The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data.

<table>
<tr>
<td></td>
<td>
PDP Context Activation Procedures
The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.
Figure 9: Call Flow for PDP Context Activation


Id. at 80.
</td>
</tr>
<tr>
<td>9[C] sending the Create PDP Context Response message from the GGSN to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the</td>
<td>
Cisco’s Mobile Multimedia Gateway Platform practices a method that comprises sending the Create PDP Context Response message from the GGSN to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below in Step 6, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address (public or private depending on the APN request) assigned to the mobile station.

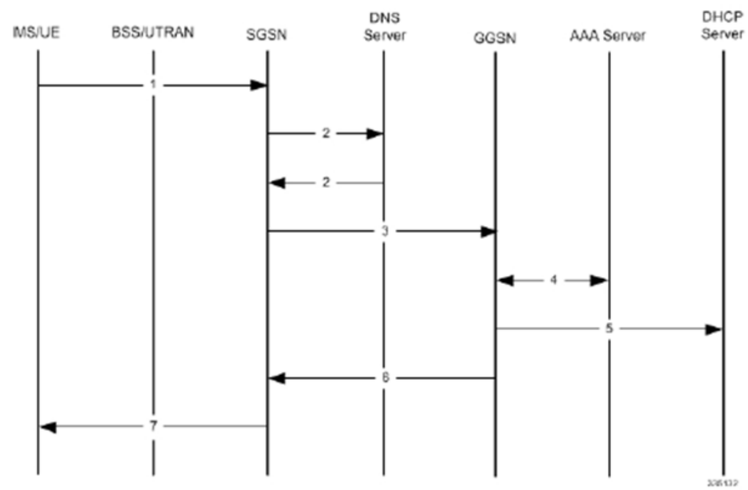
<table>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>information contained in the APN field of the Create PDP Context Request message.</td>
<td>
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>

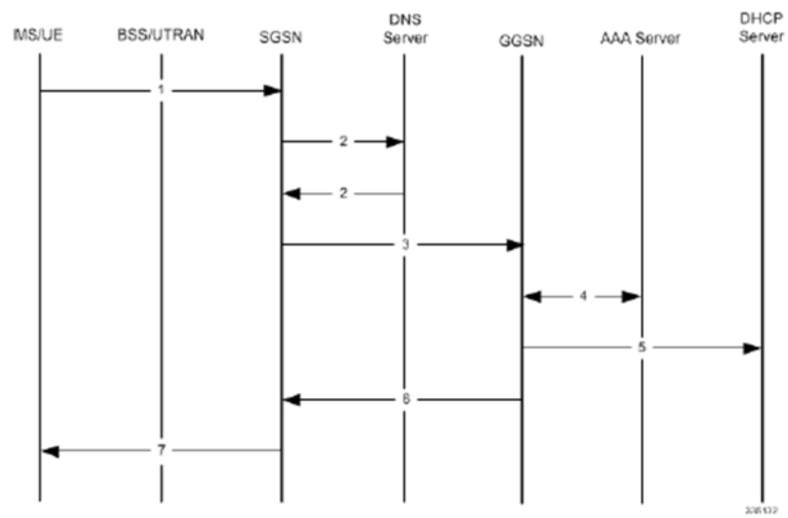
Id. at 80.
</td>
</tr>
</table>

<table>
<tr><td colspan="2">CLAIM 10</td></tr>
<tr><td>10[Pre.] A method comprising:</td><td>To any extent the preamble is limiting, Cisco’s Mobile Multimedia Gateway Platform practices a method comprising the following elements, as illustrated below.</td></tr>
<tr><td>10[A] receiving a Create Packet Data Protocol (PDP) Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN) at a Border Gateway (BG), the Create PDP Context Request Message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of a network;</td><td>Cisco’s Mobile Multimedia Gateway Platform practices a method that comprises receiving a Create Packet Data Protocol (PDP) Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN) at a Border Gateway (BG), the Create PDP Context Request Message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of a network.

StarOS includes both “Standalone gateway GPRS support node (GGSN)” and “Co-located P-GW/GGSN” deployments and interfaces. On information and belief, Cisco’s Mobile Multimedia Gateway Platform practices a method that includes receiving a Create PDP Context Request message from a Gateway General Packet Radio System (GPRS) Support Node (GGSN) at a Border Gateway (i.e., Packet Gateway: P-GW). See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).

For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. The SGSN sends an APN Restriction value (Maximum APN Restriction) in the Create PDP Context Request for establishing a PDP context.

<table><tr><td>3</td><td>The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.</td></tr></table>
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).</td></tr>
</table>

	SGSN and Dual Access SGSN Deployments SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on *System Configuration Options*, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services. *Id*. at 5. **PDP Context Activation Procedures** The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection. *Figure 9: Call Flow for PDP Context Activation*  The following table provides detailed explanations for each step indicated in the figure above. *Table 3: PDP Context Activation Procedure* **Step** — **Description** 1 — The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN). *Id*. at 80.

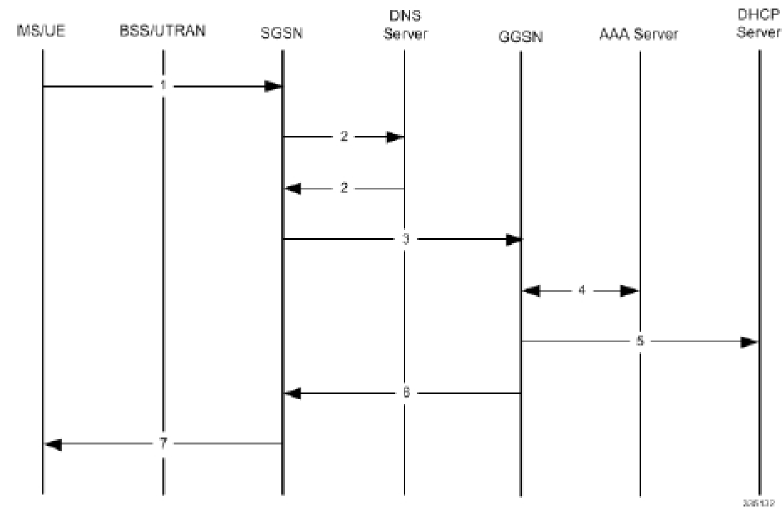
<table>
<tr>
<td></td>
<td>The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, “[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be “0” in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68).” Id. at 184.</td>
</tr>
<tr>
<td>10[B] assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message and</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices a method that comprises assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below, the mobile station is assigned an IP address (public or private) based on the information contained in the APN field of the Create PDP Context Request message.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5</td><td>If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.</td></tr>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
<tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address.

Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions.

A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr>
</table>
</td>
</tr>
</table>

	See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021). **PDP Context Activation Procedures** The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection. *Figure 9: Call Flow for PDP Context Activation*  *Id*. at 80.
10[C] sending the Create PDP Context Response message from the BG to the SGSN containing the information assigning either a	Cisco's Mobile Multimedia Gateway Platform practices a method that comprises sending the Create PDP Context Response message from the BG to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message. StarOS includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces." On information and belief, the Border Gateway (i.e., Packet Gateway: P-GW) sends the

<table>
<tr>
<td>private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.</td>
<td>Create PDP Context Response message to the SGSN. See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).

For example, as shown below in Step 6, the SGSN is sent a Create PDP Context Response message containing the IP address (public or private depending on the APN request) assigned to the mobile station.

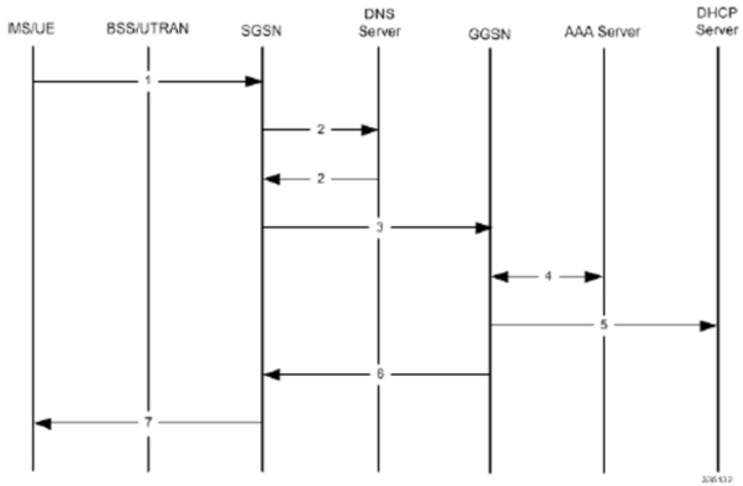
<table>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
</table>

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).</td>
</tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

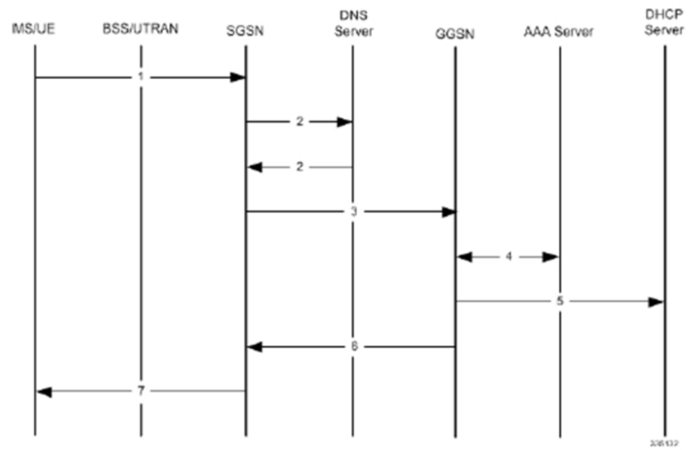
Id. at 80.

CLAIM 11

11[Pre.] A method comprising:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform practices a method that comprises the following elements, as illustrated below.

<table>
<tr>
<td>11[A] sending an Activate Packet Data Protocol (PDP) Context Request message to a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network from a mobile station of the network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station; and</td>
<td>
Cisco’s Mobile Multimedia Gateway Platform practices a method that comprises sending an Activate Packet Data Protocol (PDP) Context Request message to a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network from a mobile station of the network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station.

For example, as shown in Step 1, the SGSN receives a PDP Activation Request message from a mobile station (MS) containing an APN field.

PDP Context Activation Procedures
The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.
Figure 9: Call Flow for PDP Context Activation


The following table provides detailed explanations for each step indicated in the figure above.
Table 3: PDP Context Activation Procedure
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>
Id. at 80.

The APN Restriction value determines the type of application data the subscriber can send. For example, the “APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum
</td>
</tr>
</table>

	APN Restriction of the UE to the GGSN/P-GW in a Create PDP Context Request/Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/Create Session Request." *Id*. at 183. The APN Restriction values explicitly indicate the request for a private or public network address to be assigned to the mobile station. For example, when the "APN Restriction Value allowed to be established" is "1" then the "Private" APN for Corporate is assigned in the exemplary manner shown below. ***Table 13: APN restriction values*** (table below) *Id*. at 184. "Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured." *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 104 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool:

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value allowed to be established
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (for example MMS subscribers)	1
4	Private-2	Corporate (for example non-MMS subscribers)	None

<table>
<tr>
<td></td>
<td>
Step 1 Create the IP pool for IPv4 addresses in system context by applying the example configuration in the IPv4 Pool Creation section.
Step 2 Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the IPv6 Pool Creation section.
Step 3 Verify your IP pool configuration by following the steps in the IP Pool Configuration Verification section.
Step 4 Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Id. at 105.

IPv4 Pool Creation
Use the following example to create the IPv4 address pool:
configure
    context <dest_ctxt_name>
      ip pool <pool_name> <ip_address/mask> [{private| public}[priority]] | static]
      end

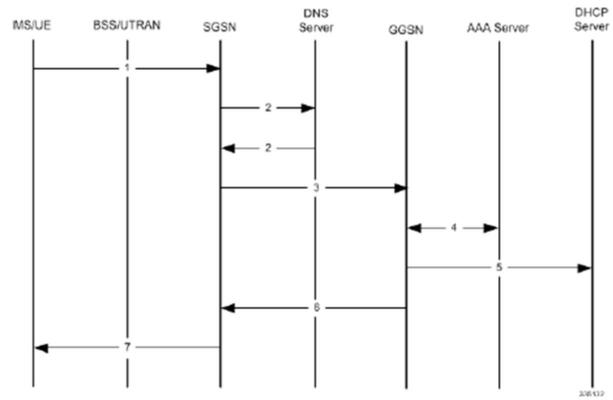
Id. at 106.
</td>
</tr>
<tr>
<td>11[B] receiving at the mobile station an Activate PDP Context Accept message containing information relating to an assignment of either a private network address or a public network address to the mobile station based on the information contained in the APN field of the</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices a method that comprises receiving at the mobile station an Activate PDP Context Accept message containing information relating to an assignment of either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.</td>
</tr>
</table>

Activate PDP Context Request message.	(see below)

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

For example, as shown below in Step 7, the SGSN sends the Activate PDP Context Accept message to the mobile station (MS) along with the IP Address.

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address.

Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions.

A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr>
</table>

Id. at 81.

The GGSN already has an APN Restriction value for each APN request by UE/MS. The GGSN checks whether the APN Restriction value received in the Create PDP Context Request from the SGSN and the APN Restriction value of the APN to which access is requested are the same. If the values are the same, the GGSN creates the PDP context and sends a create response message back to the SGSN containing the IP address assigned to the UE/MS. The SGSN then sends an Activate PDP Context Accept message to the UE/MS.

For example, “[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be “0” in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68).” Id. at 184.
</td>
</tr>
<tr>
<td colspan="2">CLAIM 12</td>
</tr>
<tr>
<td>12[A] The method according to claim 11, wherein the private network address and the</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 11, see supra 11[Pre.]-11[B], wherein the private network address and the public network address are each one of an IPv4 network address and an IPv6 network address.</td>
</tr>
</table>

<table>
<tr>
<td>public network address are each one of an IPv4 network address and an IPv6 network address.</td>
<td>For example, Cisco’s Mobile Multimedia Gateway Platform practices a method of creating an IP pool for IPv4 addresses in system context and configuring the IP pool for IPv6 addresses in system context.

Step 1 Create the IP pool for IPv4 addresses in system context by applying the example configuration in the IPv4 Pool Creation section.
Step 2 Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the IPv6 Pool Creation section.
Step 3 Verify your IP pool configuration by following the steps in the IP Pool Configuration Verification section.
Step 4 Save your configuration as described in the Verifying and Saving Your Configuration chapter.

See GGSN Administration Guide, StarOS Release 21.3, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 105 (April 27, 2017) (last accessed June 20, 2021).

IPv4 Pool Creation
Use the following example to create the IPv4 address pool:
configure
context <dest_ctxt_name>
ip pool <pool_name> <ip_address/mask> [{private| public}[priority]] | static]
end

Id. at 106.</td>
</tr>
<tr>
<td colspan="2">CLAIM 13</td>
</tr>
<tr>
<td>13[A] The method according to claim 11, wherein the network is a GPRS communications network.</td>
<td>Cisco’s Mobile Multimedia Gateway Platform practices the method according to claim 11, see supra 11[Pre.]-11[B], wherein the network is a GPRS communications network.

Cisco’s Mobile Multimedia Gateway Platform includes a GPRS communications network. For example: “StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to the wireless carriers. Functioning as an SGSN, the system readily handles wireless data services within 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunications System (UMTS) data networks. The SGSN also can serve as an interface between GPRS and/or UMTS networks and the 4G Evolved Packet Core (EPC) network.” See SGSN</td>
</tr>
</table>

	Administration Guide, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 5 (Aug. 29, 2019) (last accessed June 20, 2021).
CLAIM 14	
14[A] The method according to claim 11, wherein the network is a Universal Mobile Telecommunications System.	Cisco's Mobile Multimedia Gateway Platform practices the method according to claim 11, *see supra* 11[Pre.]-11[B], wherein the network is a Universal Mobile Telecommunications System. Cisco's Mobile Multimedia Gateway Platform includes a network that is a Universal Mobile Telecommunications system. For example: "StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to the wireless carriers. Functioning as an SGSN, the system readily handles wireless data services within 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunications System (UMTS) data networks. The SGSN also can serve as an interface between GPRS and/or UMTS networks and the 4G Evolved Packet Core (EPC) network." *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 5 (Aug. 29, 2019) (last accessed June 20, 2021).
CLAIM 15	
15[Pre.] An apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to perform the functions described in the following elements, as shown below.

SGSN Service Configuration Procedures

This chapter provides configuration instructions to enable the SGSN to function in GPRS (2.5G), UMTS (3G), or LTE (4G) networks. The *System Administration Guide* provides interface and system-level configuration details and the *Command Line Interface Reference* provides additional command information.

Important Please note that LTE (4G) support is only available in releases 14.0 an higher.

Important At least one packet processing card must be activated prior to configuring the first service. Procedures for configuring the packet processing card can be found in the *System Administration Guide*.

High level step-by-step service configuration procedures are provided for the following:

Id. at 118.

For example, "[t]he SGSN is designed to accommodate a very high rate of simultaneous attaches. The actual attach rate depends on the latencies introduced by the network and scaling of peers. In order to optimize the entire signaling chain, the SGSN eliminates or minimizes bottlenecks caused by large scale control signaling. For this purpose, the SGSN implements features such as an in-memory data-VLR and SuperCharger. Both IMSI and P-TMSI based attaches are supported." *Id.* at 15.

Further, "[t]he SGSN authenticates the subscriber via the authentication procedure. This procedure is invoked on attaches, PDP activations, inter-SGSN routing Area Updates (RAUs), and optionally by configuration for periodic RAUs. The procedure requires the SGSN to retrieve authentication quintets/triplets from the HLR (AuC) and issuing an authentication and ciphering request to the MN. The SGSN implements an in-memory data-VLR functionality to pre-fetch and store authentication vectors from the HLR. This decreases latency of the control procedures." *Id.* at 16.

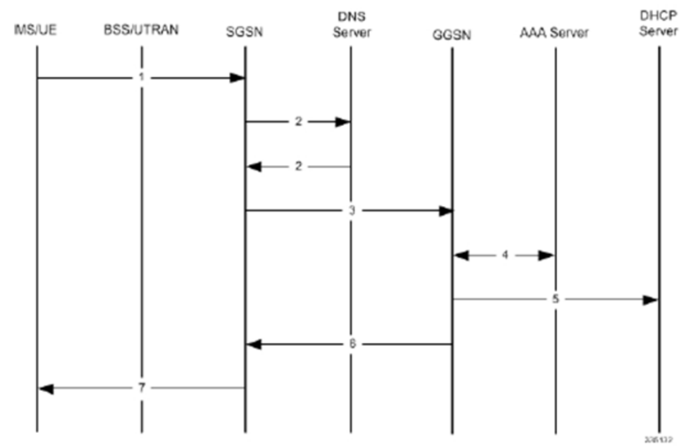
	IPv4 Pool Creation Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name>* *<ip_address/mask>* **[{private| public}[priority]] | static]** **end** Notes: • To ensure proper operation, IP pools should be configured within a destination context. • Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed. *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 106 (April 27, 2017) (last accessed June 20, 2021).
15[A] receive an Activate Packet Data Protocol (PDP) Context Request message from a mobile station of a network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network	Cisco's Mobile Multimedia Gateway Platform includes an apparatus configured to receive an Activate Packet Data Protocol (PDP) Context Request message from a mobile station of a network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station. For example, as shown below in Step 1, the SGSN receives a PDP Activation Request message from a mobile station (MS) containing an APN field.

address or a public network address to be assigned to the mobile station; and

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

The APN Restriction value determines the type of application data the subscriber can send. For example, the "APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum APN Restriction of the UE to the GGSN/P-GW in a Create PDP Context Request/Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/Create Session Request." *Id*. at 183.

The APN Restriction values explicitly indicate the request for a private or public network address to be assigned to the mobile station. For example, when the "APN Restriction Value allowed to be established" is "1" then the "Private" APN for Corporate is assigned in the exemplary manner shown below.

Table 13: APN restriction values

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value allowed to be established
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (for example MMS subscribers)	1
4	Private-2	Corporate (for example non-MMS subscribers)	None

Id. at 184.

"Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured." *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 104 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool:

Step 1 Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.

Step 2 Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.

Step 3 Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

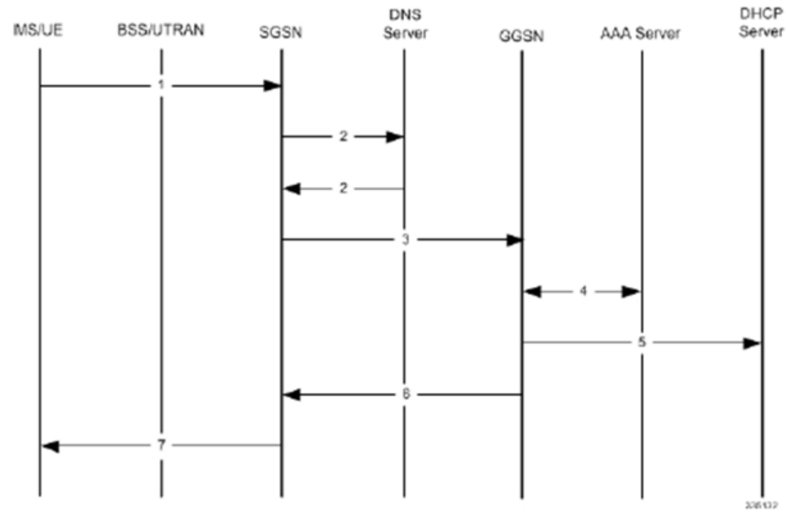
Id. at 105.

15[B] send an Activate PDP Context Accept message to the mobile station containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.	Cisco's Mobile Multimedia Gateway Platform includes an apparatus configured to send an Activate PDP Context Accept message to the mobile station containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message. For example, as shown below in Step 7, the SGSN sends the Activate PDP Context Accept message to the mobile station (MS) along with the IP Address. 7 — The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data. *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

The GGSN already has an APN Restriction value for each APN request by UE/MS. The GGSN checks whether the APN Restriction value received in the Create PDP Context Request from the SGSN and the APN Restriction value of the APN to which access is requested are the same. If the values are the same, the GGSN creates the PDP context and sends a create response message back to the SGSN containing the IP address assigned to the UE/MS. The SGSN then sends an Activate PDP Context Accept message to the UE/MS.

	For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id*. at 184.
CLAIM 16	
16[A] The apparatus according to claim 15, wherein the instructions, when executed, the apparatus is configured to: send a Create PDP Context Request to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of the network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, *see supra* 15[Pre.]-15[B], wherein the instructions, when executed, the apparatus is configured to: send a Create PDP Context Request to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of the network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network address for the mobile station. For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. The SGSN sends an APN Restriction value (Maximum APN Restriction) in the Create PDP Context Request for establishing a PDP context. 3 | The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context. *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

network address or a public network address for the mobile station; and

SGSN and Dual Access SGSN Deployments

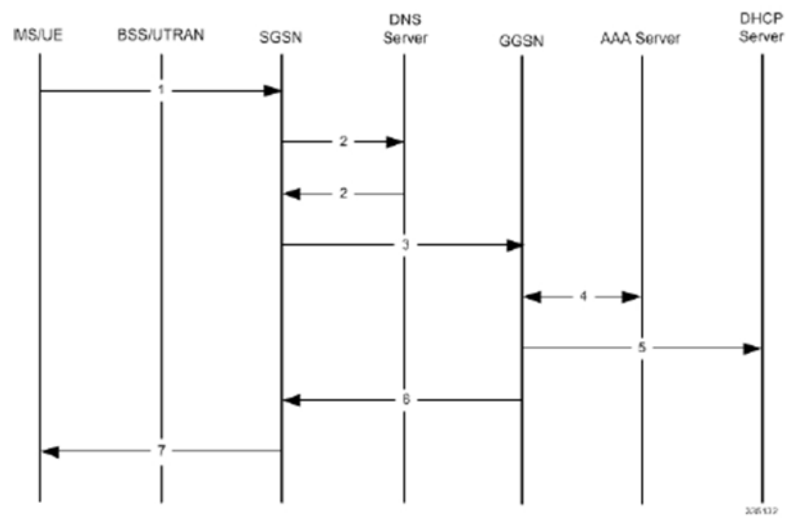
SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on *System Configuration Options*, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services.

Id. at 5.

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

<table>
<tr>
<td></td>
<td>The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, “[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be “0” in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68).” Id. at 184.</td>
</tr>
<tr>
<td>16[B] receive a Create PDP Context Response message from the GGSN containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.</td>
<td>Cisco’s Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, see supra 15[Pre.]-15[B], wherein the apparatus is configured to receive a Create PDP Context Response message from the GGSN containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.

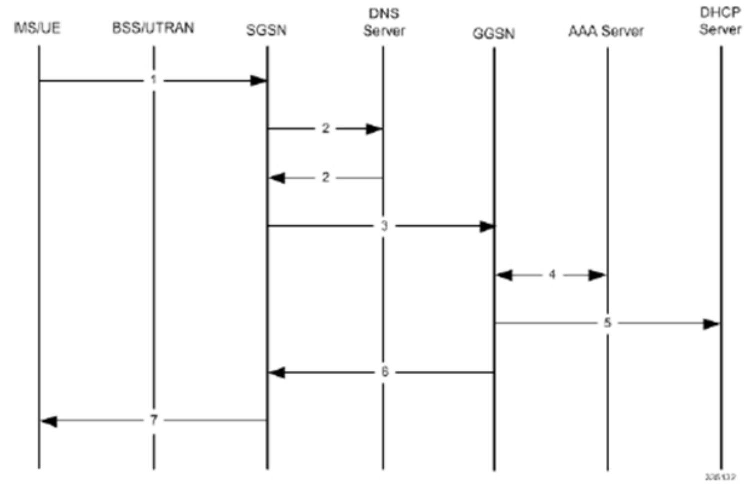
For example, as shown below in Step 6, once an IP address (public or private depending on the APN request) is chosen, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address assigned to the mobile station.

<table><tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr></table>
Id. at 81.</td>
</tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

CLAIM 17	
17[A] The apparatus according to claim 15, wherein the instructions, when executed, the	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, *see supra* 15[Pre.]-15[B], wherein the instructions, when executed, the apparatus is configured to: send a Create Packet Data Protocol (PDP) Context Request message to a Border Gateway (BG) of a network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network address for the mobile station.

apparatus is configured to: send a Create Packet Data Protocol (PDP) Context Request message to a Border Gateway (BG) of a network, the Create PDP Context Request message having an APN field containing information relating to a request for either a private network address or a public network address for the mobile station; and	For example, Cisco's Mobile Multimedia Gateway Platform includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, Cisco's Mobile Multimedia Gateway Platform sends a Create PDP Context Request message to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) or to a Border Gateway (Packet Gateway: P-GW). *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021). Further to this example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id.* at 184.
17[B] receive a Create PDP Context Response message from the BG containing information assigning either a private network address or a public network address to the mobile station based on the information	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, *see supra* 15[Pre.]-15[B], wherein the apparatus is configured to receive a Create PDP Context Response message from the BG containing information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message. For example, StarOS includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, Cisco's Mobile Multimedia Gateway Platform is configured to receive a Create PDP Context Response message from a Gateway General Packet Radio System (GPRS) Support Node (GGSN) or a Border Gateway (Packet Gateway: P-GW). *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).

contained in the APN field of the Activate PDP Context Request message.	
CLAIM 18	
18[A] The apparatus according to claim 15, wherein the private network address and the public network address are each one of an IPv4 network address and an IPv6 network address.	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, *see supra* 15[Pre.]-15[B], wherein the private network address and the public network address are each one of an IPv4 network address and an IPv6 network address. For example, Cisco's Mobile Multimedia Gateway Platform practices a method of creating an IP pool for IPv4 addresses in system context and configuring the IP pool for IPv6 addresses in system context. **Step 1** Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section. **Step 2** Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section. **Step 3** Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section. **Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter. *See GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 105 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool: **IPv4 Pool Creation** Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name>* *<ip_address/mask>* **[{private| public}[priority]] | static]** **end** *Id*. at 106.

CLAIM 19	
19[A] The apparatus according to claim 15, wherein the network is a GPRS communications network.	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, *see supra* 15[Pre.]-15[B], wherein the network is a GPRS communications network. Cisco's Mobile Multimedia Gateway Platform includes a GPRS communications network. For example: "StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to the wireless carriers. Functioning as an SGSN, the system readily handles wireless data services within 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunications System (UMTS) data networks. The SGSN also can serve as an interface between GPRS and/or UMTS networks and the 4G Evolved Packet Core (EPC) network." *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 5 (Aug. 29, 2019) (last accessed June 20, 2021).
CLAIM 20	
20[A] The apparatus according to claim 15, wherein the network is a Universal Mobile Telecommunications System.	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, *see supra* 15[Pre.]-15[B], wherein the network is a Universal Mobile Telecommunications System. Cisco's Mobile Multimedia Gateway Platform includes a network that is a Universal Mobile Telecommunications system. For example: "StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to the wireless carriers. Functioning as an SGSN, the system readily handles wireless data services within 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunications System (UMTS) data networks. The SGSN also can serve as an interface between GPRS and/or UMTS networks and the 4G Evolved Packet Core (EPC) network." *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 5 (Aug. 29, 2019) (last accessed June 20, 2021).

<table>
<tr><th colspan="2">CLAIM 21</th></tr>
<tr><td>21[A] The apparatus according to claim 15, wherein the information comprises one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station.</td><td>Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 15, see supra 15[Pre.]-15[B], wherein the information comprises one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station.

For example, the APN Restriction value determines the type of application data the subscriber can send. The "APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum APN Restriction of the UE to the GGSN/P-GW in a Create PDP Context Request/Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/Create Session Request." See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 5 (Aug. 29, 2019) (last accessed June 20, 2021).

The APN Restriction values explicitly indicate the request for a private or public network address to be assigned to the mobile station. For example, when the "APN Restriction Value allowed to be established" is "1," then the "Private" APN for Corporate is assigned in the exemplary manner shown below.

Table 13: APN restriction values
<table><tr><th>Maximum APN Restriction Value</th><th>Type of APN</th><th>Application Example</th><th>APN Restriction Value allowed to be established</th></tr><tr><td>0</td><td colspan="2">No Existing Contexts or Restriction</td><td>All</td></tr><tr><td>1</td><td>Public-1</td><td>WAP or MMS</td><td>1, 2, 3</td></tr><tr><td>2</td><td>Public-2</td><td>Internet or PSPDN</td><td>1, 2</td></tr><tr><td>3</td><td>Private-1</td><td>Corporate (for example MMS subscribers)</td><td>1</td></tr><tr><td>4</td><td>Private-2</td><td>Corporate (for example non-MMS subscribers)</td><td>None</td></tr></table>
Id. at 184.</td></tr>
</table>

	"Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured." *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 104 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool: **Step 1** Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section. **Step 2** Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section. **Step 3** Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section. **Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter. *Id*. at 105. **IPv4 Pool Creation** Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name>* *<ip_address/mask>* **[{private| public}[priority]] | static]** **end** *Id*. at 106.
CLAIM 22	
22[Pre.] An apparatus comprising a processor and a memory storing instructions that,	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to perform the functions described below.

when executed, the apparatus is configured to:	**SGSN Service Configuration Procedures** This chapter provides configuration instructions to enable the SGSN to function in GPRS (2.5G), UMTS (3G), or LTE (4G) networks. The *System Administration Guide* provides interface and system-level configuration details and the *Command Line Interface Reference* provides additional command information. **Important** Please note that LTE (4G) support is only available in releases 14.0 an higher. **Important** At least one packet processing card must be activated prior to configuring the first service. Procedures for configuring the packet processing card can be found in the *System Administration Guide*. High level step-by-step service configuration procedures are provided for the following: *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 118 (Aug. 29, 2019) (last accessed June 20, 2021). For example, "[t]he SGSN is designed to accommodate a very high rate of simultaneous attaches. The actual attach rate depends on the latencies introduced by the network and scaling of peers. In order to optimize the entire signaling chain, the SGSN eliminates or minimizes bottlenecks caused by large scale control signaling. For this purpose, the SGSN implements features such as an in-memory data-VLR and SuperCharger. Both IMSI and P-TMSI based attaches are supported." *Id.* at 15. Further, "[t]he SGSN authenticates the subscriber via the authentication procedure. This procedure is invoked on attaches, PDP activations, inter-SGSN routing Area Updates (RAUs), and optionally by configuration for periodic RAUs. The procedure requires the SGSN to retrieve authentication quintets/triplets from the HLR (AuC) and issuing an authentication and ciphering request to the MN. The SGSN implements an in-memory data-VLR functionality to pre-fetch and store authentication vectors from the HLR. This decreases latency of the control procedures." *Id.*, at 16.

	IPv4 Pool Creation Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name>* *<ip_address/mask>* **[{private| public}[priority]] | static]** **end** Notes: • To ensure proper operation, IP pools should be configured within a destination context. • Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed. *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 106 (April 27, 2017) (last accessed June 20, 2021).
22[A] receive a Create Packet Data Protocol (PDP) Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN), the Create PDP Context Request Message having an APN (Access Point Name) field containing information that	Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to receive a Create Packet Data Protocol (PDP) Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN), the Create PDP Context Request Message having an APN (Access Point Name) field containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of a network. For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. The SGSN sends an APN Restriction value (Maximum APN Restriction) in the Create PDP Context Request for establishing a PDP context. <table><tr><td>3</td><td>The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.</td></tr></table>

<table>
<tr>
<td>explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of a network;</td>
<td>

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

SGSN and Dual Access SGSN Deployments

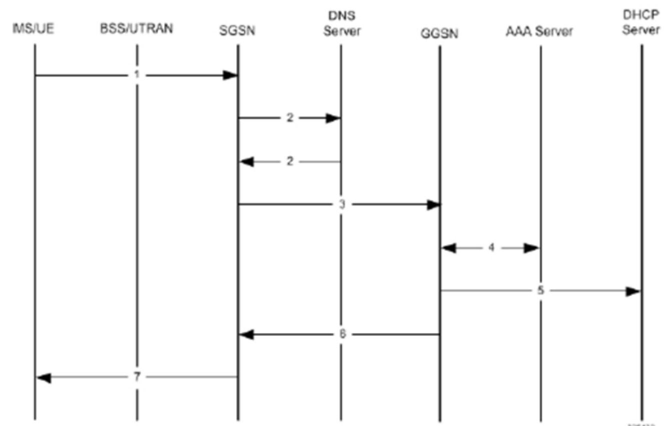
SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on *System Configuration Options*, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services.

Id. at 5.

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>

Id. at 80.

</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, “[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be “0” in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68).” Id. at 184.</td>
</tr>
<tr>
<td>22[B] assign either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message; and</td>
<td>Cisco’s Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to assign either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below, the mobile station is assigned an IP address (public or private) based on the information contained in the APN field of the Create PDP Context Request message.

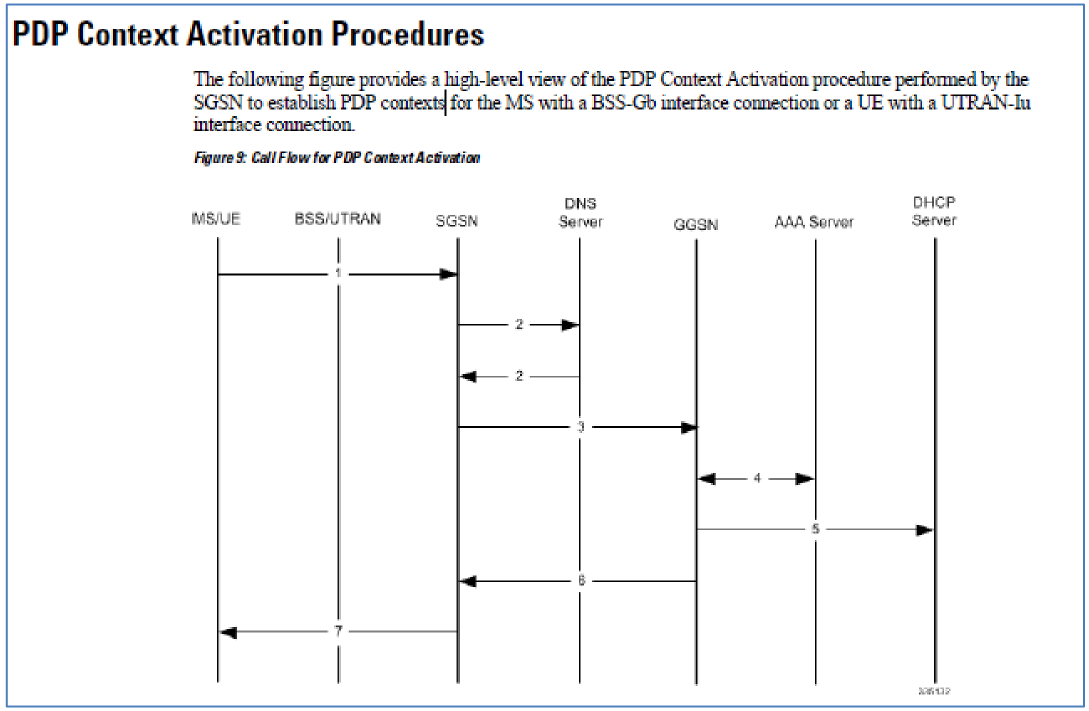
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5</td><td>If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.</td></tr>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
<tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address.

Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions.

A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>

See SGSN Administration Guide, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).



PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation

Id. at 80.

</td>
</tr>
<tr>
<td>

22[C] send the Create PDP Context Response message to the SGSN containing the information assigning either a

</td>
<td>

Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to send the Create PDP Context Response message to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below in Step 6, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address (public or private depending on the APN request) assigned to the mobile station.

</td>
</tr>
</table>

private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

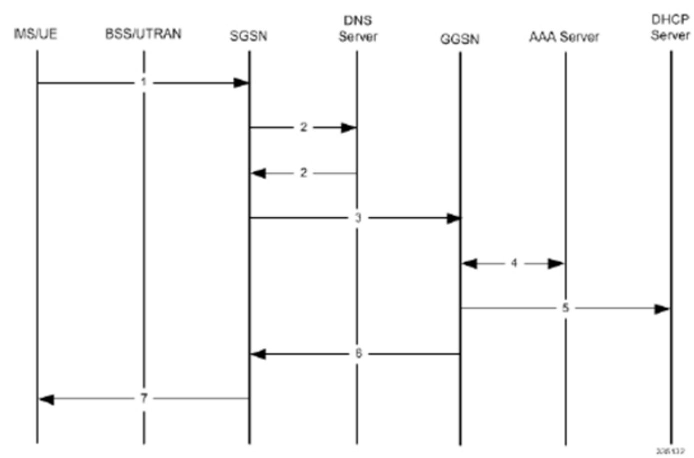
6	The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

CLAIM 23	
23[Pre.] An apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to:	To any extent the preamble is limiting, Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to perform the functions described below. **SGSN Service Configuration Procedures** This chapter provides configuration instructions to enable the SGSN to function in GPRS (2.5G), UMTS (3G), or LTE (4G) networks. The *System Administration Guide* provides interface and system-level configuration details and the *Command Line Interface Reference* provides additional command information. **Important** Please note that LTE (4G) support is only available in releases 14.0 an higher. **Important** At least one packet processing card must be activated prior to configuring the first service. Procedures for configuring the packet processing card can be found in the *System Administration Guide*. High level step-by-step service configuration procedures are provided for the following: *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 118 (Aug. 29, 2019) (last accessed June 20, 2021). For example, "[t]he SGSN is designed to accommodate a very high rate of simultaneous attaches. The actual attach rate depends on the latencies introduced by the network and scaling of peers. In order to optimize the entire signaling chain, the SGSN eliminates or minimizes bottlenecks caused by large scale control signaling. For this purpose, the SGSN implements features such as an in-memory data-VLR and SuperCharger. Both IMSI and P-TMSI based attaches are supported." *Id.* at 15.

	Further, "[t]he SGSN authenticates the subscriber via the authentication procedure. This procedure is invoked on attaches, PDP activations, inter-SGSN routing Area Updates (RAUs), and optionally by configuration for periodic RAUs. The procedure requires the SGSN to retrieve authentication quintets/triplets from the HLR (AuC) and issuing an authentication and ciphering request to the MN. The SGSN implements an in-memory data-VLR functionality to pre-fetch and store authentication vectors from the HLR. This decreases latency of the control procedures." *Id.* at 16. **IPv4 Pool Creation** Use the following example to create the IPv4 address pool: **configure** **context** <*dest_ctxt_name*> **ip pool** <*pool_name*> <*ip_address/mask*> **[{private| public}[priority]] | static]** **end** Notes: • To ensure proper operation, IP pools should be configured within a destination context. • Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed. *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 106 (April 27, 2017) (last accessed June 20, 2021).
23[A] receive a Create PDP Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network, the Create PDP Context Request message	Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to receive a Create PDP Context Request message from a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network, the Create PDP Context Request message having an APN (Access Point Name)field containing one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of the network. For example, as shown in Step 3 below, the SGSN sends a Create PDP Context Request to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. The SGSN sends an APN Restriction value (Maximum APN Restriction) in the Create PDP Context Request for establishing a PDP context.

<table>
<tr>
<td>having an APN (Access Point Name) field containing one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of the network;</td>
<td>
<table>
<tr><td>3</td><td>The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.</td></tr>
</table>

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

SGSN and Dual Access SGSN Deployments

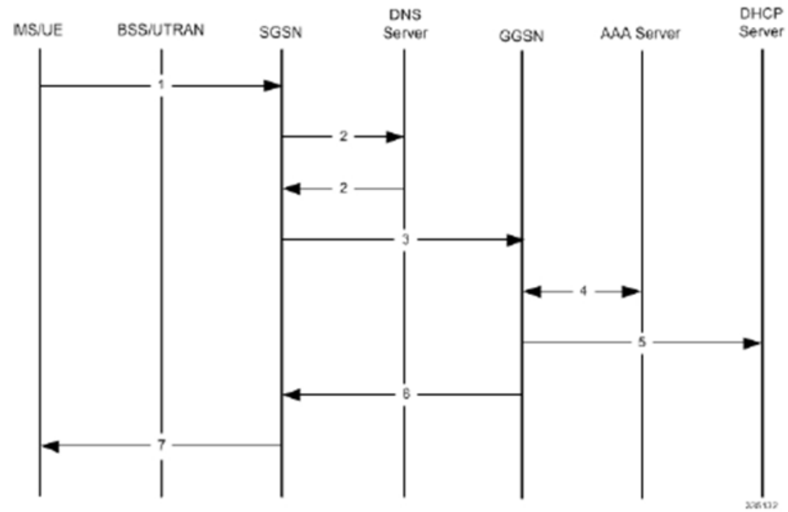
SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on System Configuration Options, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services.

Id. at 5.
</td>
</tr>
</table>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

Id. at 80.

The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value

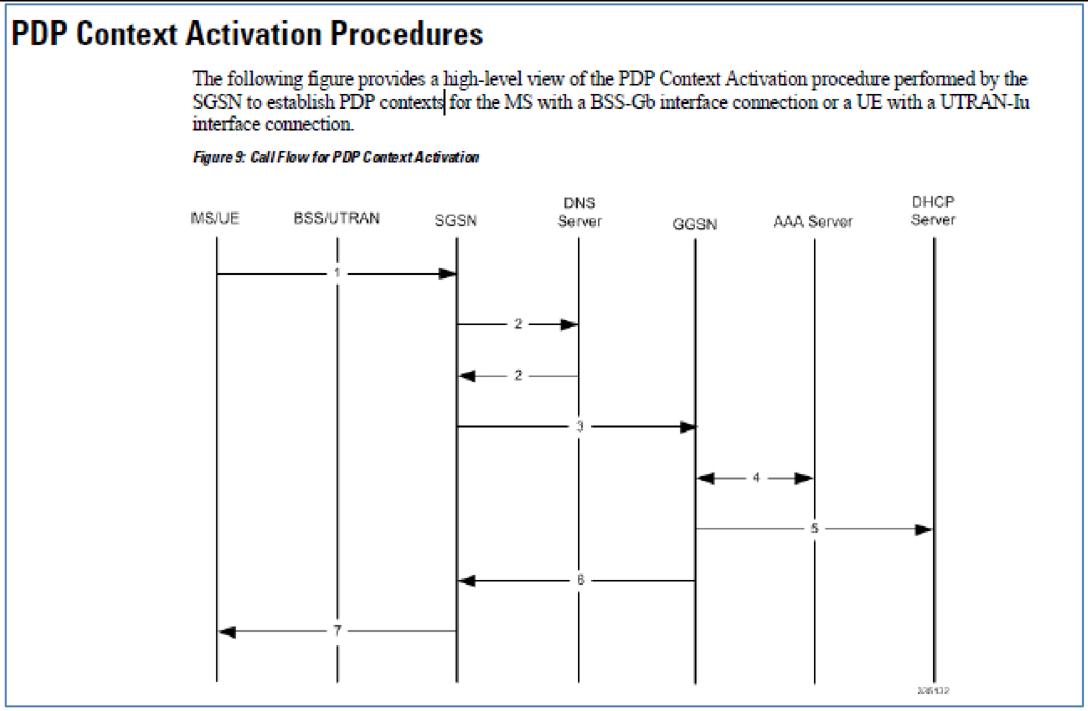
<table>
<tr>
<td></td>
<td>of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68).” Id. at 184.</td>
</tr>
<tr>
<td>23[B] assign either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message; and</td>
<td>Cisco’s Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to assign either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message.

For example, as shown below, the mobile station is assigned an IP address (public or private) based on the information contained in the APN field of the Create PDP Context Request message.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5</td><td>If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.</td></tr>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
<tr><td>7</td><td>The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address.

Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions.

A GTP-U tunnel is now established and the MS/UE can send and receive data.</td></tr>
</table>
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).</td>
</tr>
</table>

	 **PDP Context Activation Procedures** The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection. *Figure 9: Call Flow for PDP Context Activation* *Id*. at 80.
23[C] send the Create PDP Context Response message to the SGSN containing the information assigning either a private network address or a public network address to the mobile station	Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to send the Create PDP Context Response message to the SGSN containing the information assigning either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Create PDP Context Request message. For example, as shown below in Step 6, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address (public or private depending on the APN request) assigned to the mobile station.

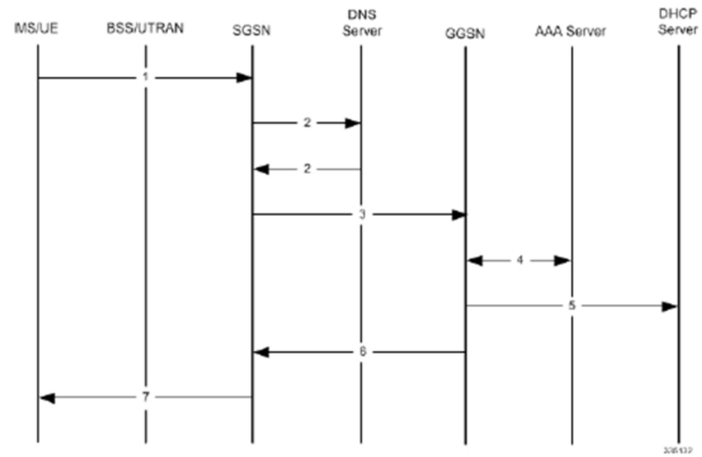
<table>
<tr>
<td>based on the information contained in the APN field of the Create PDP Context Request message.</td>
<td>
<table>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
</table>

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>

Id. at 80.
</td>
</tr>
</table>

CLAIM 24	
24[Pre.] An apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to:	Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that, when executed, the apparatus is configured to perform the functions described below. **SGSN Service Configuration Procedures** This chapter provides configuration instructions to enable the SGSN to function in GPRS (2.5G), UMTS (3G), or LTE (4G) networks. The *System Administration Guide* provides interface and system-level configuration details and the *Command Line Interface Reference* provides additional command information. **Important** Please note that LTE (4G) support is only available in releases 14.0 an higher. **Important** At least one packet processing card must be activated prior to configuring the first service. Procedures for configuring the packet processing card can be found in the *System Administration Guide*. High level step-by-step service configuration procedures are provided for the following: *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 118 (Aug. 29, 2019) (last accessed June 20, 2021). For example, "[t]he SGSN is designed to accommodate a very high rate of simultaneous attaches. The actual attach rate depends on the latencies introduced by the network and scaling of peers. In order to optimize the entire signaling chain, the SGSN eliminates or minimizes bottlenecks caused by large scale control signaling. For this purpose, the SGSN implements features such as an in-memory data-VLR and SuperCharger. Both IMSI and P-TMSI based attaches are supported." *Id.*, at 15. Further, "[t]he SGSN authenticates the subscriber via the authentication procedure. This procedure is invoked on attaches, PDP activations, inter-SGSN routing Area Updates (RAUs), and optionally by configuration for periodic

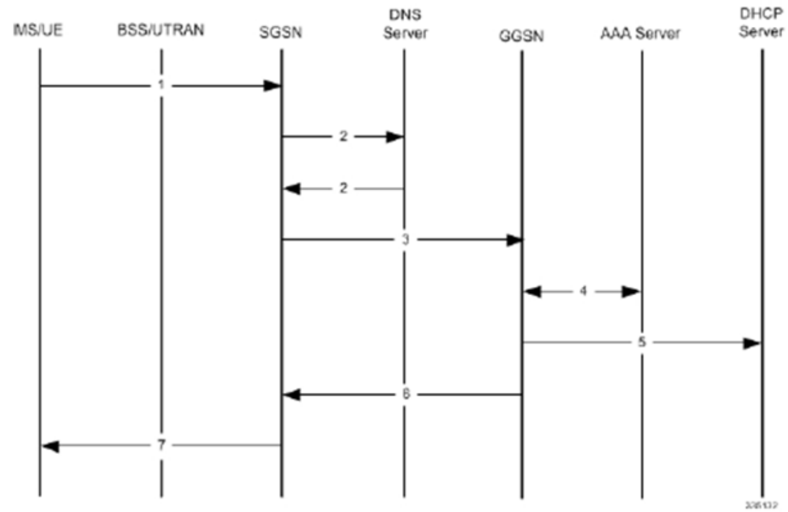
	RAUs. The procedure requires the SGSN to retrieve authentication quintets/triplets from the HLR (AuC) and issuing an authentication and ciphering request to the MN. The SGSN implements an in-memory data-VLR functionality to pre-fetch and store authentication vectors from the HLR. This decreases latency of the control procedures." *Id.*, at 16. **IPv4 Pool Creation** Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name>* *<ip_address/mask>* **[{private| public}[priority]] | static]** **end** Notes: • To ensure proper operation, IP pools should be configured within a destination context. • Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed. *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 106 (April 27, 2017) (last accessed June 20, 2021).
24[A] send an Activate Packet Data Protocol (PDP) Context Request message to a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network, the Activate PDP Context Request	Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to send an Activate Packet Data Protocol (PDP) Context Request message to a Serving General Packet Radio System (GPRS) Support Node (SGSN) of a network, the Activate PDP Context Request message having an APN (Access Point Name) field containing information containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station. For example, as shown below in Step 1, the SGSN receives a PDP Activation Request message from a mobile station (MS) containing an APN field.

<table>
<tr>
<td>message having an APN (Access Point Name) field containing information containing information that explicitly indicates requesting either a private network address or a public network address to be assigned to the mobile station; and</td>
<td>

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).

See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).

The APN Restriction value determines the type of application data the subscriber can send. For example, the "APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum APN Restriction of the UE to the GGSN/P-GW in a Create PDP Context Request/Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/Create Session Request." *Id.* at 183.

</td>
</tr>
</table>

	The APN Restriction values explicitly indicate the request for a private or public network address to be assigned to the mobile station. For example, when the "APN Restriction Value allowed to be established" is "1" then the "Private" APN for Corporate is assigned in the exemplary manner shown below.

Table 13: APN restriction values

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value allowed to be established
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (for example MMS subscribers)	1
4	Private-2	Corporate (for example non-MMS subscribers)	None

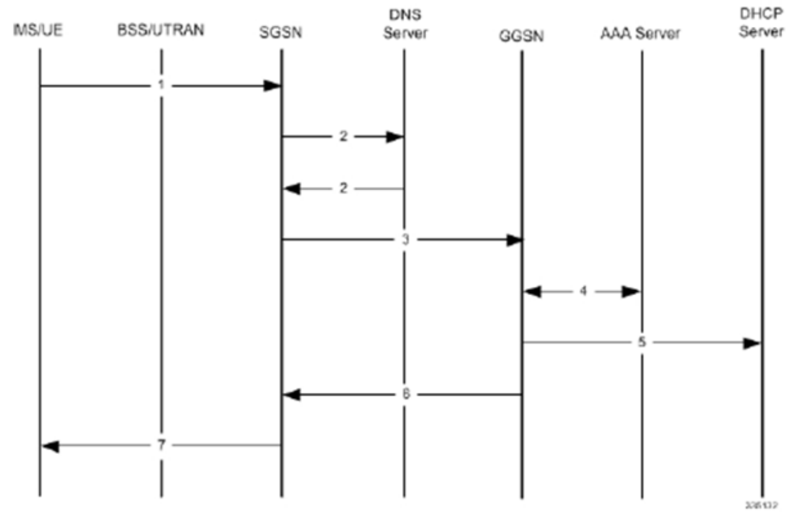
Id. at 184.

"Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured." *GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 104 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool:

Step 1	Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.
Step 2	Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.
Step 3	Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.
Step 4	Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Id. at 105.

	IPv4 Pool Creation Use the following example to create the IPv4 address pool: **configure** **context** *<dest_ctxt_name>* **ip pool** *<pool_name>* *<ip_address/mask>* **[{private| public}[priority]] | static]** **end** *Id*. at 106.
24[B] receive an Activate PDP Context Accept message containing information relating to an assignment of either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message.	Cisco's Mobile Multimedia Gateway Platform includes an apparatus comprising a processor and a memory storing instructions that is configured to receive an Activate PDP Context Accept message containing information relating to an assignment of either a private network address or a public network address to the mobile station based on the information contained in the APN field of the Activate PDP Context Request message. For example, as shown below in Step 7, the SGSN sends the Activate PDP Context Accept message to the mobile station (MS) along with the IP Address. 7 — The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data. *See SGSN Administration Guide*, *StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).

	PDP Context Activation Procedures The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection. *Figure 9: Call Flow for PDP Context Activation*  The following table provides detailed explanations for each step indicated in the figure above. *Table 3: PDP Context Activation Procedure* **Step** — **Description** 1 — The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN). *Id*. at 80. The GGSN already has an APN Restriction value for each APN request by UE/MS. The GGSN checks whether the APN Restriction value received in the Create PDP Context Request from the SGSN and the APN Restriction value of the APN to which access is requested are the same. If the values are the same, the GGSN creates the PDP context and sends a create response message back to the SGSN containing the IP address assigned to the UE/MS. The SGSN then sends an Activate PDP Context Accept message to the UE/MS.

	For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id*. at 184.
CLAIM 25	
25[A] The apparatus according to claim 24, wherein the private network address and the public network address are each one of an IPv4 network address and an IPv6 network address.	Cisco's Mobile Multimedia Gateway Platform includes the apparatus according to claim 24, *see supra* 24[Pre.]-24[B], wherein the private network address and the public network address are each one of an IPv4 network address and an IPv6 network address. For example, Cisco's Mobile Multimedia Gateway Platform practices a method of creating an IP pool for IPv4 addresses in system context and configuring the IP pool for IPv6 addresses in system context. **Step 1** Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section. **Step 2** Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section. **Step 3** Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section. **Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter. *See GGSN Administration Guide, StarOS Release 21.3*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/GGSN/21-3-GGSN-Admin.pdf, at 105 (April 27, 2017) (last accessed June 20, 2021). To configure the IP pool:

<table>
<tr><td></td><td>IPv4 Pool Creation

Use the following example to create the IPv4 address pool:

configure
    context <dest_ctxt_name>
      ip pool <pool_name> <ip_address/mask> [{private| public}[priority]] | static]
      end

Id. at 106.</td></tr>
<tr><td colspan="2">CLAIM 26</td></tr>
<tr><td>26[Pre.] A system comprising:</td><td>To any extent the preamble is limiting, Cisco’s Mobile Multimedia Gateway Platform includes a system comprising the following elements, as shown below.</td></tr>
<tr><td>26[A] a Serving General Packet Radio System (GPRS) Support Node (SGSN) configured to send a Create Packet Data Protocol (PDP) Context Request to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of a network, the Create PDP Context Request message having an APN (Access Point</td><td>Cisco’s Mobile Multimedia Gateway Platform includes a system comprising a Serving General Packet Radio System (GPRS) Support Node (SGSN) configured to send a Create Packet Data Protocol (PDP) Context Request to a Gateway General Packet Radio System (GPRS) Support Node (GGSN) of a network, the Create PDP Context Request message having an APN (Access Point Name) field containing one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of the network.

For example, as shown in Step 3 below, to resolve the received APN in the PDP activation request message, the SGSN sends a Create PDP Context Request to the GGSN, which works in conjunction with the SGSN to identify the APN the mobile station is attempting to connect to and other information about the subscriber. The SGSN sends an APN Restriction value (Maximum APN Restriction) in the Create PDP Context Request for establishing a PDP context.

<table><tr><td>3</td><td>The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.</td></tr></table>
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 80 (Aug. 29, 2019) (last accessed June 20, 2021).</td></tr>
</table>

<table>
<tr>
<td>Name) field containing one or more parameters that explicitly indicates requesting either a private network address or a public network address to be assigned to a mobile station of the network;</td>
<td>

SGSN and Dual Access SGSN Deployments

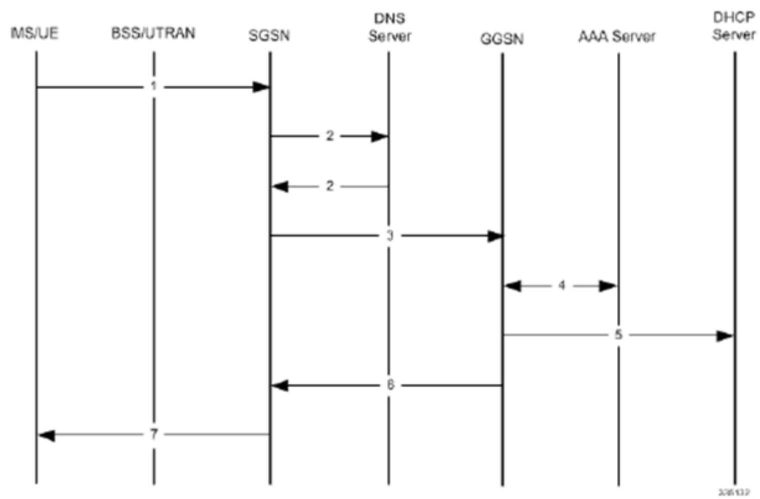
SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on *System Configuration Options*, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services.

Id. at 5.

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



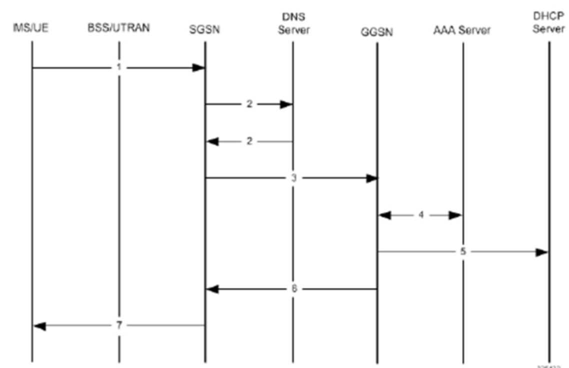
The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>

Id. at 80.
</td>
</tr>
</table>

	The SGSN sends the APN Restriction value for the UE to the GGSN in the Create PDP Context Request. For example, "[d]uring default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/P-GW in the Create PDP Context Request/Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context/Create Session Response failure message to the G/S4-SGSN with EGTP cause EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)." *Id.* at 184.
26[B] a GGSN configured to send the Create PDP Context Request message to a Border Gateway (BG); and	Cisco's Mobile Multimedia Gateway Platform includes, on information and belief, a system comprising a GGSN configured to send the Create PDP Context Request message to a Border Gateway (BG). For example, Cisco's Mobile Multimedia Gateway Platform includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, the GGSN is configured to send the Create PDP Context Request message to a Border Gateway (Packet Gateway: P-GW). *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).
26[C] a BG configured to send a Create PDP Context Response message to the GGSN,	Cisco's Mobile Multimedia Gateway Platform includes, on information and belief, a system comprising a BG configured to send a Create PDP Context Response message to the GGSN. For example, Cisco's Mobile Multimedia Gateway Platform includes both "Standalone gateway GPRS support node (GGSN)" and "Co-located P-GW/GGSN" deployments and interfaces. On information and belief, the Border Gateway (Packet Gateway: P-GW) is configured to send the Create PDP Context Response message to the GGSN. *See SGSN Administration Guide, StarOS Release 21.15*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 6-7 (Aug. 29, 2019) (last accessed June 20, 2021).

<table>
<tr>
<td>26[D] the SGSN configured to receive the Create PDP Context Response from the GGSN.</td>
<td>
Cisco's Mobile Multimedia Gateway Platform includes a system wherein the SGSN is configured to receive the Create PDP Context Response from the GGSN.
For example, as shown below in Step 6, once an IP address (public or private depending on the APN request) is chosen, the GGSN sends a Create PDP Context Response message to the SGSN containing the IP address assigned to the mobile station.
<table>
<tr><td>6</td><td>The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.</td></tr>
</table>
See SGSN Administration Guide, StarOS Release 21.15, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-15_6-9/SGW-Admin/21-15-SGSN-Admin.pdf, at 81 (Aug. 29, 2019) (last accessed June 20, 2021).
PDP Context Activation Procedures
The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.
Figure 9: Call Flow for PDP Context Activation


The following table provides detailed explanations for each step indicated in the figure above.
Table 3: PDP Context Activation Procedure
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).</td></tr>
</table>
Id. at 80.
</td>
</tr>
</table>

EXHIBIT C

EXHIBIT C

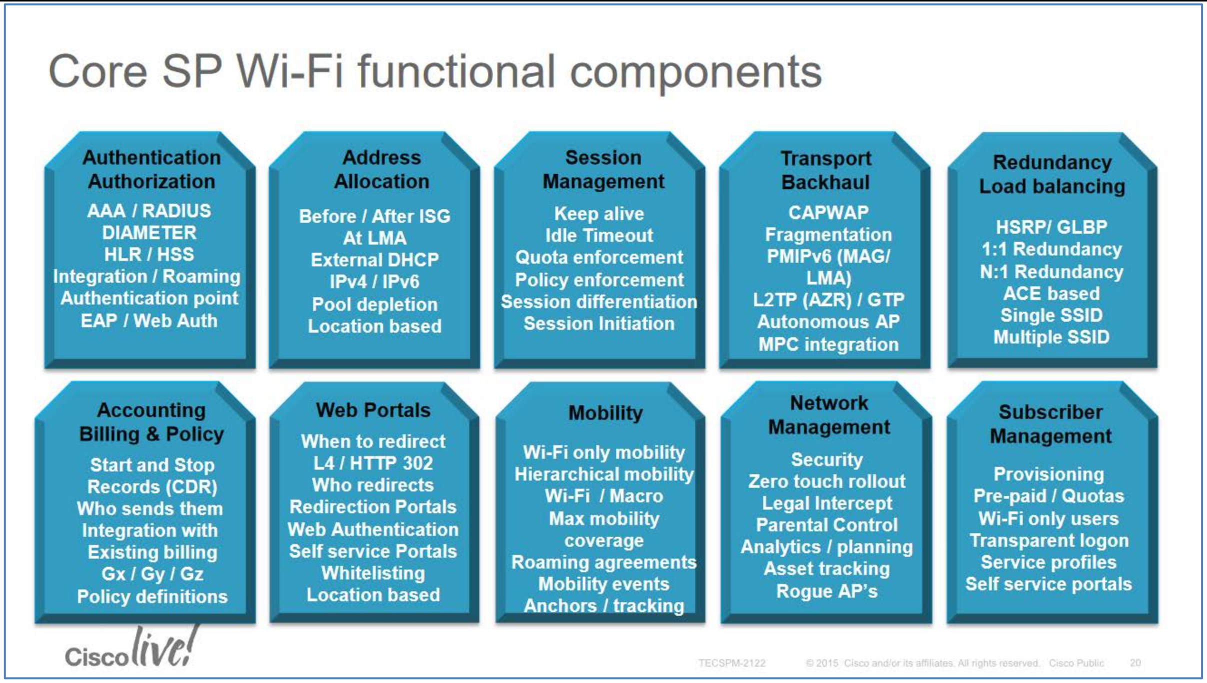
U.S. Patent No. 8,191,106 v. Cisco Service Provider Wi-Fi Product Portfolio

U.S. Patent No. 8,191,106	Application to Cisco Service Provider Wi-Fi Product Portfolio
CLAIM 1	
1[Pre.] A system for network access security policy management of multimodal access to a converged network, the system comprising:	To any extent the preamble is limiting, the Cisco Service Provider Wi-Fi product portfolio ("Cisco's SP Wi-Fi")[1] provides a system for network access security policy management of multimodal access to a converged network. Cisco's SP Wi-Fi is used to provide a system for network access security policy management of multimodal access to a converged network, comprising various hardware elements including, but not limited to, Access Points (Aps), Wireless Controllers (WLCs), Wireless Access Gateways (WAGs), Packet Gateways (PGWs), PCRFs (Policy and Charging Rule Functions), and PCEFs (Policy and Charging Enforcement Functions). *See End-to-End Service Provider Wi-Fi Solutions*, CISCO, TECSPM-2122, at 19 (hereinafter "*TECSPM*").

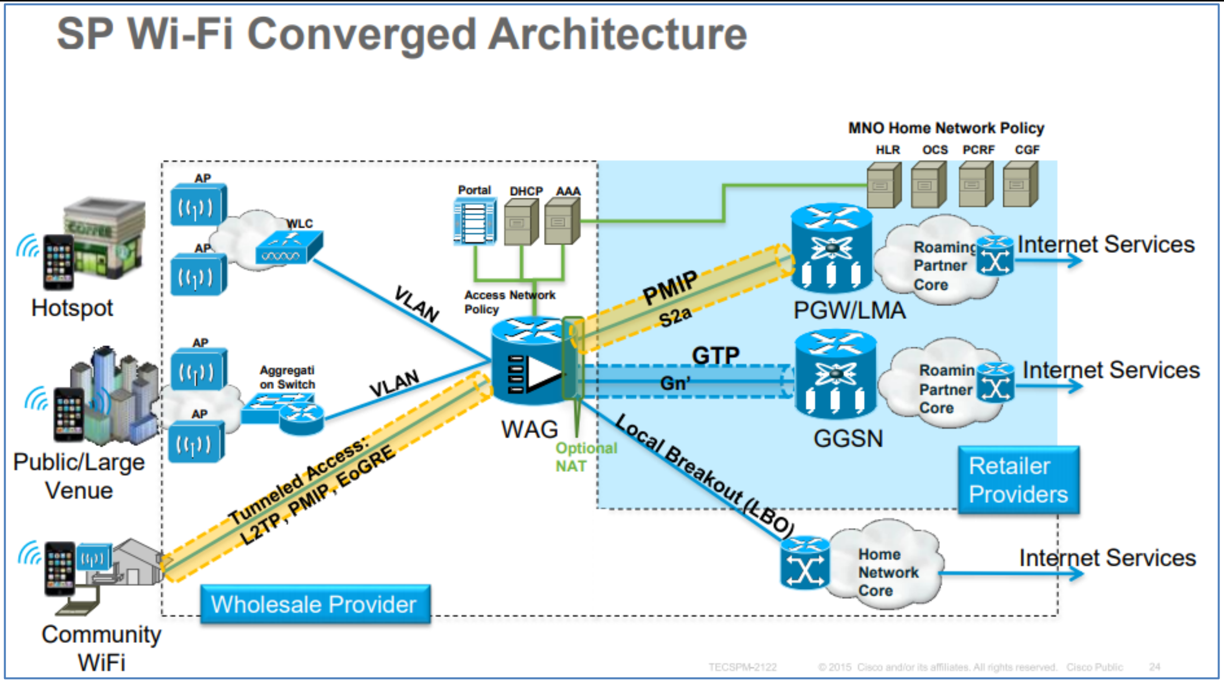
[1] This portfolio includes, but is not limited to, the Cisco Cloud Services Router 1000V Series, Cisco 1000 Series Aggregation Services Routers, Cisco ASR 9000 Series Aggregation Services Routers, Cisco 5500 Series Wireless Controllers, Cisco 8500 Series Wireless Controllers, Cisco Virtual Wireless Controller, and Cisco Aironet 1530, 1550, and 1570 Series Outdoor Access Points.

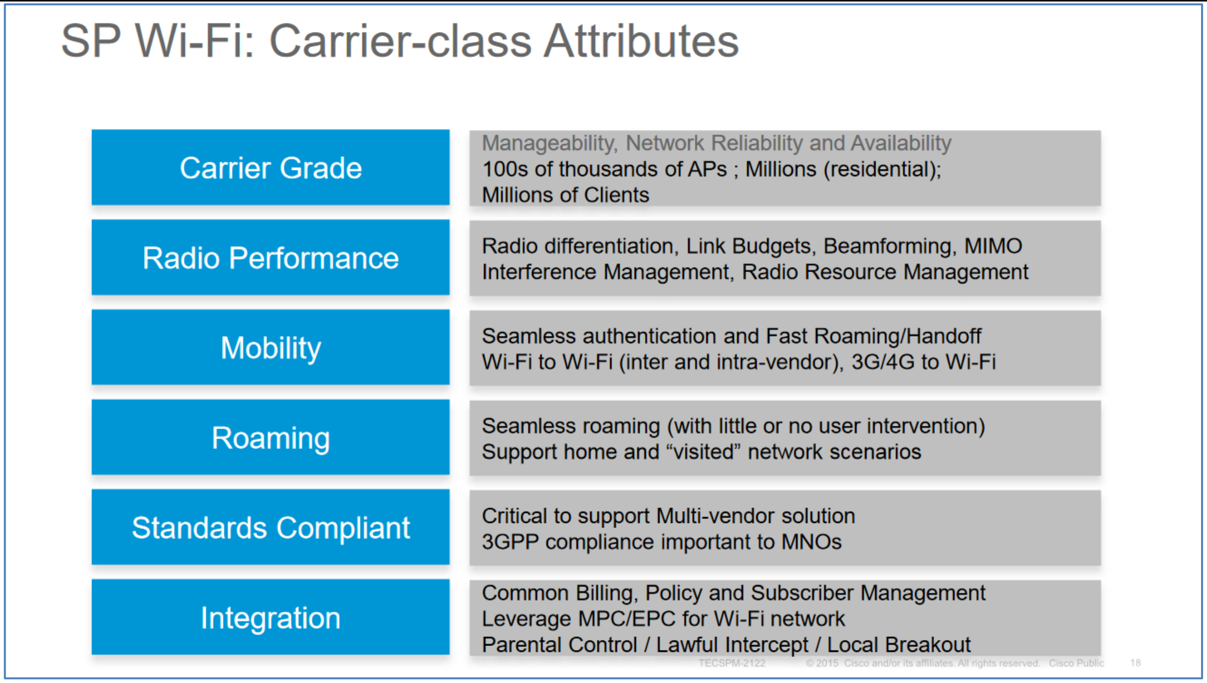

Cisco E2E Product Portfolio for SP Wi-Fi
WAG, GGSN, PGW, ePDG, TTG:
Cisco ASR5500/ASR5700
WAG & ISG:
Cisco ASR1000/9000/CSR1000v
Indoor Access Points:
Cisco Aironet 1700/2700/3700 Series
Outdoor Access Points:
Cisco Aironet 1532/1552/1572 Series
Wireless LAN Controllers:
Cisco 5500/8500/vWLC
WLAN Management:
Cisco Prime Infrastructure (CPI)
AAA:
Cisco Prime Access Registrar (CPAR)
Server:
Cisco UCS
Ciscolive!
TECSPM-2122
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public
19

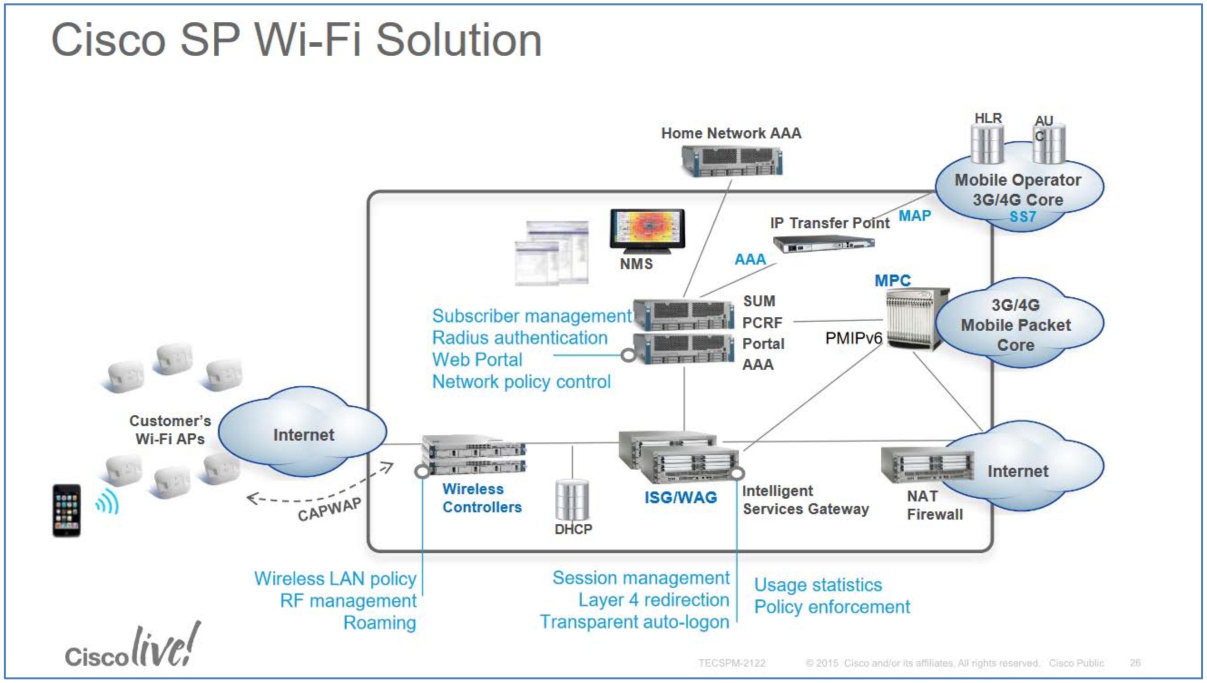
Id. at 19.


Core SP Wi-Fi functional components
Authentication Authorization
AAA / RADIUS
DIAMETER
HLR / HSS
Integration / Roaming
Authentication point
EAP / Web Auth
Address Allocation
Before / After ISG
At LMA
External DHCP
IPv4 / IPv6
Pool depletion
Location based
Session Management
Keep alive
Idle Timeout
Quota enforcement
Policy enforcement
Session differentiation
Session Initiation
Transport Backhaul
CAPWAP
Fragmentation
PMIPv6 (MAG/ LMA)
L2TP (AZR) / GTP
Autonomous AP
MPC integration
Redundancy Load balancing
HSRP/ GLBP
1:1 Redundancy
N:1 Redundancy
ACE based
Single SSID
Multiple SSID
Accounting Billing & Policy
Start and Stop Records (CDR)
Who sends them
Integration with Existing billing
Gx / Gy / Gz
Policy definitions
Web Portals
When to redirect
L4 / HTTP 302
Who redirects
Redirection Portals
Web Authentication
Self service Portals
Whitelisting
Location based
Mobility
Wi-Fi only mobility
Hierarchical mobility
Wi-Fi / Macro
Max mobility coverage
Roaming agreements
Mobility events
Anchors / tracking
Network Management
Security
Zero touch rollout
Legal Intercept
Parental Control
Analytics / planning
Asset tracking
Rogue AP's
Subscriber Management
Provisioning
Pre-paid / Quotas
Wi-Fi only users
Transparent logon
Service profiles
Self service portals
Cisco live!
TECSPM-2122
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public
20

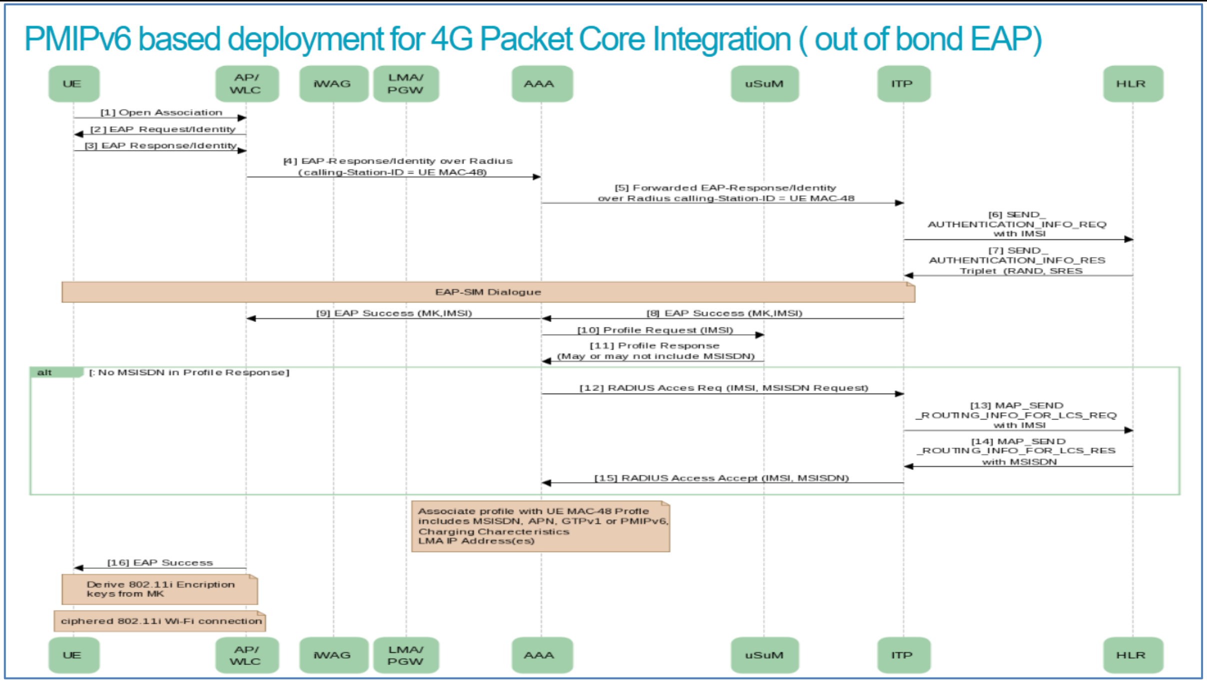
Id. at 20.

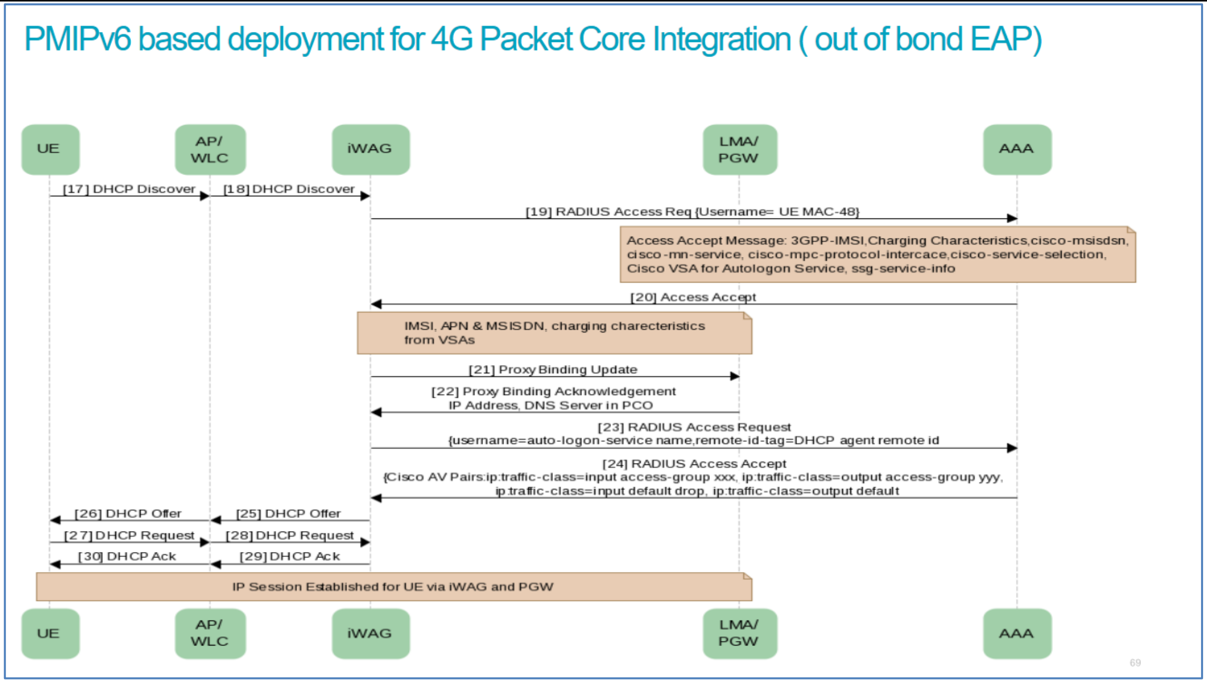
	 *Id.* at 24. Cisco's SP Wi-Fi provides seamless and efficient handoff between access technologies (e.g., 3G/4G to Wi-Fi) as well as offering policy and subscriber management features.

	 *Id*. at 18.
1[A] an inter-technology change-off monitoring entity (ICME) for detecting an inter-technology change-off of a multimodal device from a first access technology of the converged network to a second access technology of	Cisco's SP Wi-Fi system comprises an inter-technology change-off monitoring entity (ICME) for detecting an inter-technology change-off of a multimodal device from a first access technology of the converged network to a second access technology of the converged network, and for transmitting an inter-technology change-off message. Cisco SP Wi-Fi APs or WLCs (e.g., "an inter-technology change-off monitoring entity (ICME)") are connected to by user equipment (UE). The ICME detects the inter-technology change-off of the UE (e.g., "a multimodal device") from a first access technology (e.g., 3G/4G) of the converged network to a second access technology (e.g., Wi-Fi) of the converged network and transmits a Dynamic Host Configuration Protocol

the converged network, and for transmitting an inter-technology change-off message;	(DHCP) message[2] (e.g., an "inter-technology change-off message"). *TECSPM* at 26, 68-69 (disclosing Cisco's UE to WLAN handover (e.g., "inter-technology change-off of a multimodal device from a first access technology of the converged network to a second access technology of the converged network") process in the Cisco SP Wi-Fi system).  *Id*. at 26.

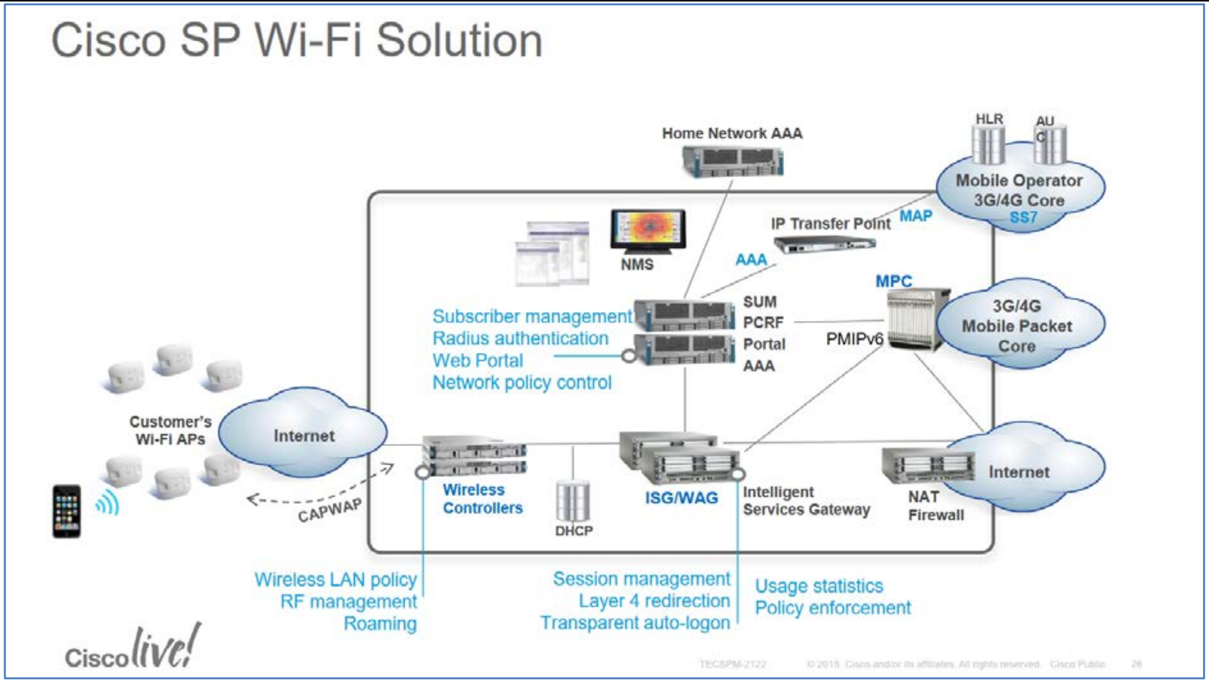
[2] "When a host boots up, the TCP/IP stack in the host transmits a broadcast (DHCPDISCOVER) message in order to gain an IP address and subnet mask, among other configuration parameters. This initiates an exchange between the DHCP server and the host." The use of the DHCPDISCOVER message is that the client is "looking for available DHCP servers." *See Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, CISCO, https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html (updated Nov. 17, 2008, last accessed Mar. 10, 2021). Put another way, the DHCPDISCOVER's purpose is for a client to discover available servers and their offered network functionality.

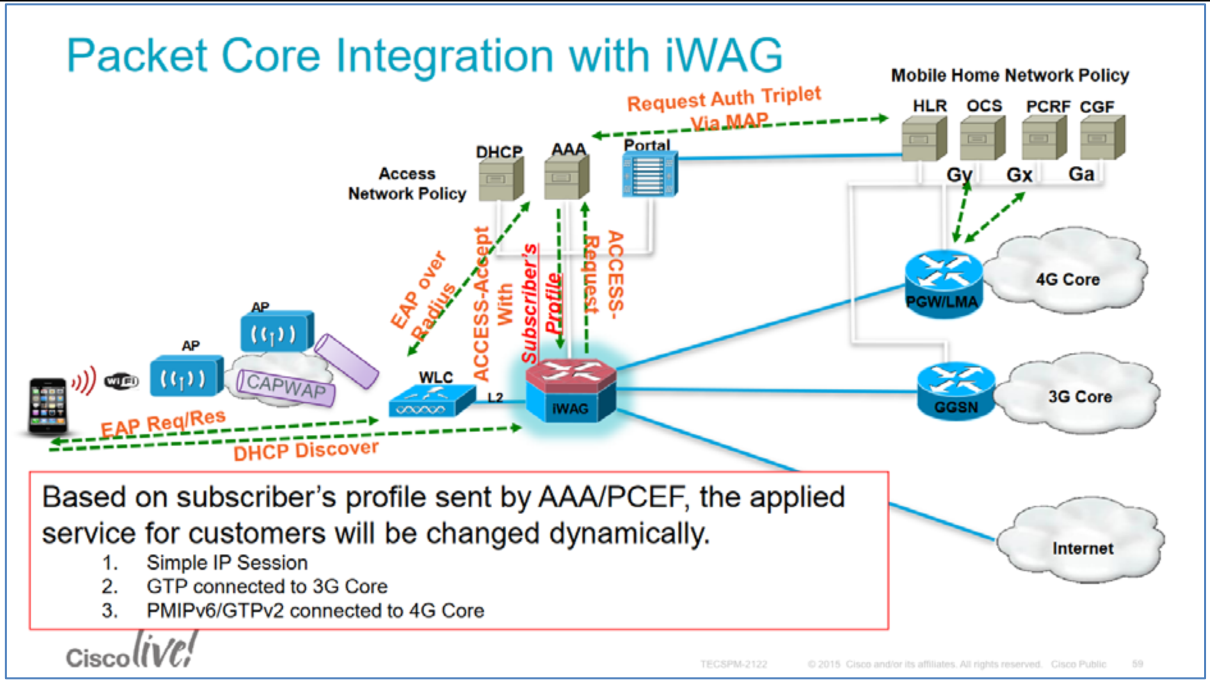
	PMIPv6 based deployment for 4G Packet Core Integration (out of bond EAP) UE AP/ WLC iWAG LMA/ PGW AAA uSuM ITP HLR [1] Open Association [2] EAP Request/Identity [3] EAP Response/Identity [4] EAP-Response/Identity over Radius (calling-Station-ID = UE MAC-48) [5] Forwarded EAP-Response/Identity over Radius calling-Station-ID = UE MAC-48 [6] SEND_ AUTHENTICATION_INFO_REQ with IMSI [7] SEND_ AUTHENTICATION_INFO_RES Triplet (RAND, SRES EAP-SIM Dialogue [9] EAP Success (MK,IMSI) [8] EAP Success (MK,IMSI) [10] Profile Request (IMSI) [11] Profile Response (May or may not include MSISDN) alt [: No MSISDN in Profile Response] [12] RADIUS Acces Req (IMSI, MSISDN Request) [13] MAP_SEND _ROUTING_INFO_FOR_LCS_REQ with IMSI [14] MAP_SEND _ROUTING_INFO_FOR_LCS_RES with MSISDN [15] RADIUS Access Accept (IMSI, MSISDN) Associate profile with UE MAC-48 Profle includes MSISDN, APN, GTPv1 or PMIPv6, Charging Charecteristics LMA IP Address(es) [16] EAP Success Derive 802.11i Encription keys from MK ciphered 802.11i Wi-Fi connection *Id*. at 68.

<table>
<tr>
<td></td>
<td>


Id. at 69.
</td>
</tr>
<tr>
<td>1[B] a policy database for storing a plurality of access technology policies; and</td>
<td>Cisco's SP Wi-Fi comprises a policy database for storing a plurality of access technology policies.

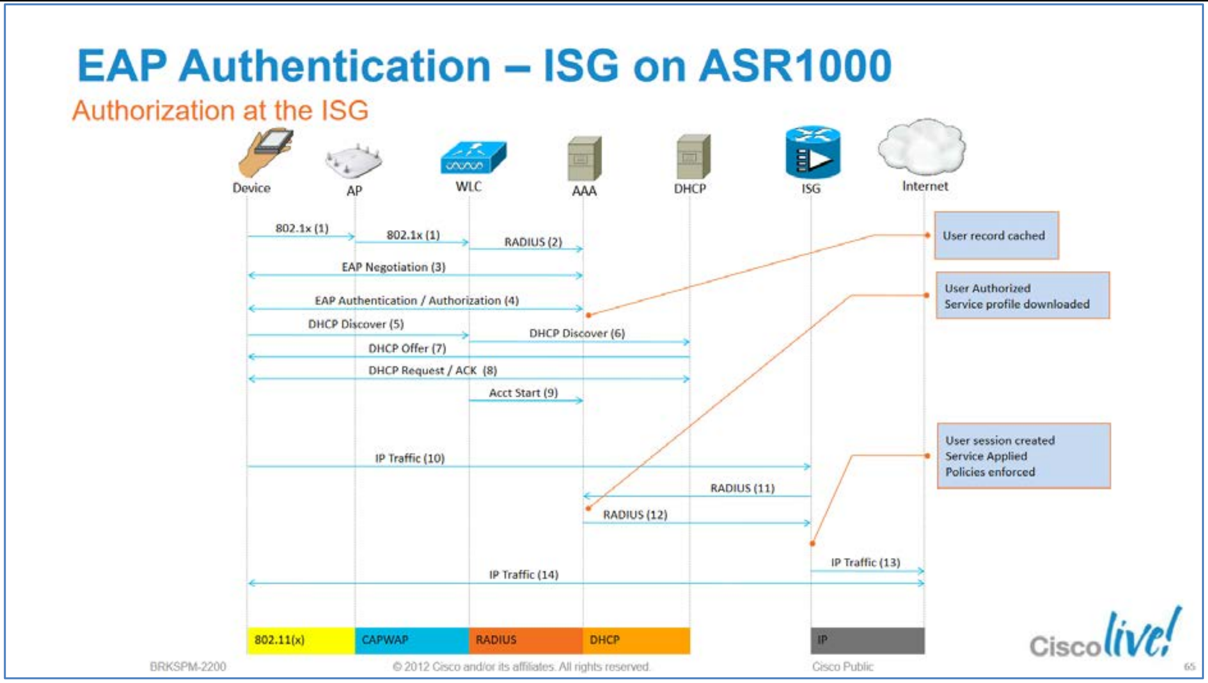
As one example, Cisco's SP Wi-Fi integrates WAGs with PCRFs and Authentication, Authorization, and Accounting (AAA) servers (e.g., "a policy database") which store subscriber profiles (e.g., "a plurality of access technology policies").</td>
</tr>
</table>

	 *See TECSPM* at 26 (providing an overview of policy management).

	 *Id.* at 59 (describing how subscriber profiles (*e.g.*, "access technology policies") affect applied service for customers).
1[C] a policy manager for receiving said inter-technology change-off message from the ICME, for searching said policy database for an access technology policy corresponding to	Cisco's SP Wi-Fi system comprises a policy manager for receiving said inter-technology change-off message from the ICME, for searching said policy database for an access technology policy corresponding to said second access technology, for determining appropriate policies to be enforced, and for distributing said appropriate policies to at least one policy enforcement point (PEF) for enforcing said appropriate policies in respect of access by the multimodal device to the converged network. Cisco's SP Wi-Fi utilizes one or more Intelligent Wireless Access Gateways (iWAGs) (e.g., "a policy manager for receiving said inter-technology change-off message from the ICME"), aware of ISG subscriber awareness through a connection to AAA servers or PCRF (e.g., "searching said policy database for an access technology policy corresponding to said second access technology, for determining appropriate policies to be enforced, and for distributing said appropriate policies to at least one policy enforcement point (PEF) for enforcing said

said second access technology, for determining appropriate policies to be enforced, and for distributing said appropriate policies to at least one policy enforcement point (PEF) for enforcing said appropriate policies in respect of access by the multimodal device to the converged network,	appropriate policies in respect of access by the multimodal device to the converged network"), to enable 3G/4G offloading to Wi-Fi. *See Intelligent Wireless Access Gateway Configuration Guide*, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iwag/configuration/xe-16/IWAG_Config_Guide_BookMap/iwag-overview.html (last accessed June 18, 2021). Service providers use a combination of WiFi and mobility offerings to offload their mobility networks in the area of high-concentration service usage. This led to the evolution of the Intelligent Wireless Access Gateway (iWAG). The iWAG provides a WiFi offload option to 4G and 3G service providers by enabling a single-box solution that provides the combined functionality of Proxy Mobile IPv6 (PMIPv6) and GPRS Tunneling Protocol (GTP) on the Cisco Intelligent Services Gateway (Cisco ISG) framework. This document provides information about the iWAG and how to configure it, and contains the following sections: Further, Cisco's Policy Enforcement Points (PEPs per Cisco documentation; PEFs per the '106 patent) are a component of policy-based management (e.g., "distributing said appropriate policies to at least one policy enforcement point (PEF) for enforcing said appropriate policies in respect of access by the multimodal device to the converged network") implementable by Cisco's ISGs or iWAGs. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 200 (last accessed June 18, 2021).

	At install time, you need to determine what policy enforcement points your installation use and what features you need to install. PEPS might be: • Cisco ISG pool • Cisco ASR 5K • Cisco ASR9K • MAG • IWAG • Cisco WLC • SCE Device Pool • RADIUS AAA server or device pool • Procera • Allot • PDSN • PCEF Consult your Cisco technical representative for configuring a custom site. *Id.* at 200. A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however. Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource. *Id.* at 199 (discussing how Cisco's PDPs determine appropriate policies to be enforced).



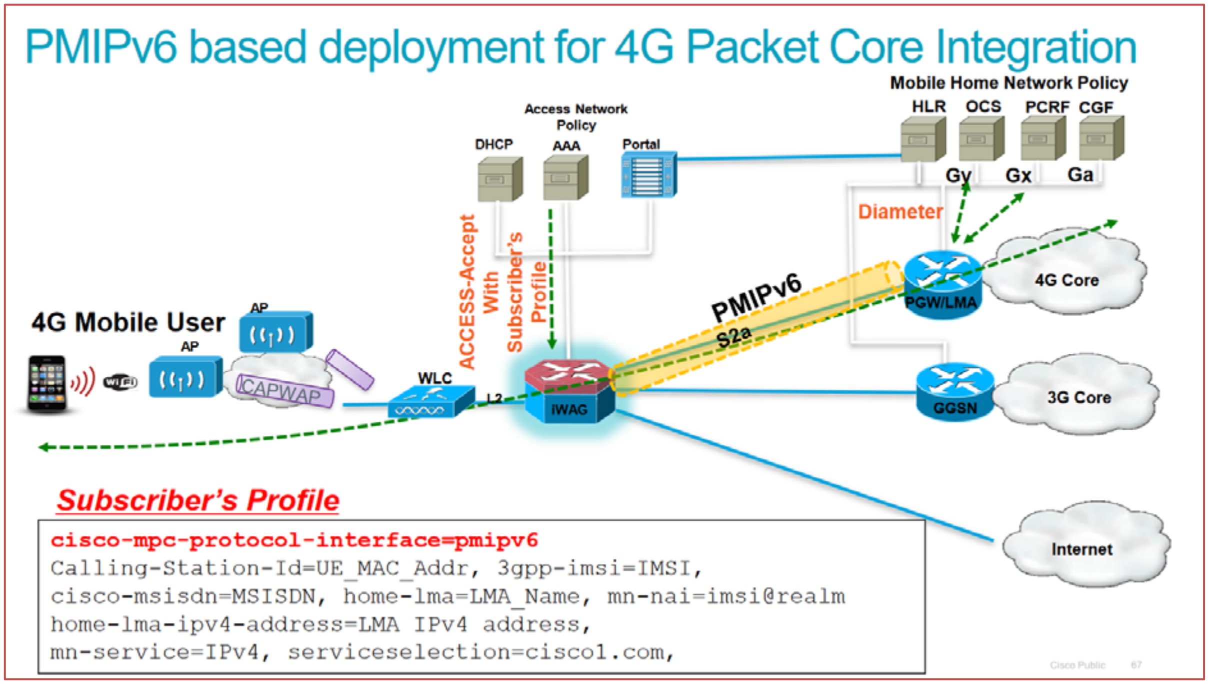
See SP WiFi: Deploying Access for 3G and 4G Mobile Networks, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 65 (last accessed June 18, 2021) (describing ISG authorization flow).

1[D] wherein at least one of the ICME and the policy manager is implemented in hardware.	Cisco's SP Wi-Fi system comprises a system wherein at least one of the ICME and the policy manager is implemented in hardware. At least one of Cisco's SP Wi-Fi APs and/or WLCs (e.g., "ICME") and Cisco's ISGs and/or WAGs (e.g., "policy manager") is implemented in physical network hardware.

<table>
<tr><td></td><td>


TECSPM at 19.
</td></tr>
<tr><td colspan="2">CLAIM 2</td></tr>
<tr><td>2[A] A system according to claim 1 wherein said inter-technology change-off message comprises a user ID identifying a subscriber, and at least one of a device</td><td>Cisco's SP Wi-Fi provides a system according to claim 1 wherein said inter-technology change-off message comprises a user ID identifying a subscriber, and at least one of a device ID, a second access technology indicator, and a first access technology indicator.

Cisco's SP Wi-Fi subscriber profiles include a cisco-msisdn attribute (e.g., "a user ID identifying a subscriber") and a Calling-Station-Id attribute (e.g., "at least one of a device ID"). Additionally, on information and belief, Cisco's SP Wi-Fi subscriber profiles includes a Cisco-Service-Selection attribute ("a second access technology indicator") and ("a first access technology indicator"). See Cisco Wireless Controller Configuration Guide,</td></tr>
</table>

ID, a second access technology indicator, and a first access technology indicator.	*Release 8.2*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_0101010.html (updated Sep. 16, 2020, last accessed June 18, 2021).  *See TECSPM* at 67 (generally describing subscriber profile structure for 4G Packet Core).
CLAIM 3	
3[A] A system according to claim 2 wherein said policy manager is further for looking up, in a subscriber database,	Cisco's SP Wi-Fi provides a system according to claim 2 wherein said policy manager is further for looking up, in a subscriber database, subscriber security parameters of a subscriber identified in the inter-technology change-off message, and for searching said policy database for a user policy corresponding to said subscriber. Cisco's SP Wi-Fi iWAG(s) look up, in subscriber profile repository (SPR), subscriber security parameters of a subscriber identified in a DHCP message.

subscriber security parameters of a subscriber identified in the inter-technology change-off message, and for searching said policy database for a user policy corresponding to said subscriber.	**Revised: February 24, 2013, OL-29745-03** Cisco Policy Suite adapts to a variety of sources for subscriber data. Possible subscriber profile repositories (SPR) that may be available to you are: • Cisco Control Center interface component of CPS • Cisco's Unified Subscriber Manager (Cisco Unified SuM) component of CPS • Cisco's AAA server component of CPS • LDAP • AAA This flexibility lets you include either an external subscriber management system in your Cisco Policy Builder architecture or the internal, integrated Cisco Unified SuM. Subscriber management schemes vary and are particular to an individual network. Because of this, the procedures for obtaining subscriber data are discussed in the specific documents that matches your network architecture. See your specific document. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 209 (last accessed June 18, 2021).

<table>
<tr>
<td></td>
<td>Further, Cisco’s iWAG(s) search a policy database for a user policy corresponding to said subscriber.

> A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however.

> Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource.

See id. at 199.</td>
</tr>
<tr>
<td colspan="2">CLAIM 5</td>
</tr>
<tr>
<td>5[A] A system according to claim 1 wherein the ICME is one of a layer 2 monitoring entity and a higher than layer 2 monitoring entity.</td>
<td>Cisco’s SP Wi-Fi provides a system according to claim 1 wherein the ICME is one of a layer 2 monitoring entity and a higher than layer 2 monitoring entity.

Cisco’s SP Wi-Fi APs and/or WLCs (e.g., “ICME”) constitute one of a layer 2 monitoring entity and a higher than layer 2 monitoring entity.

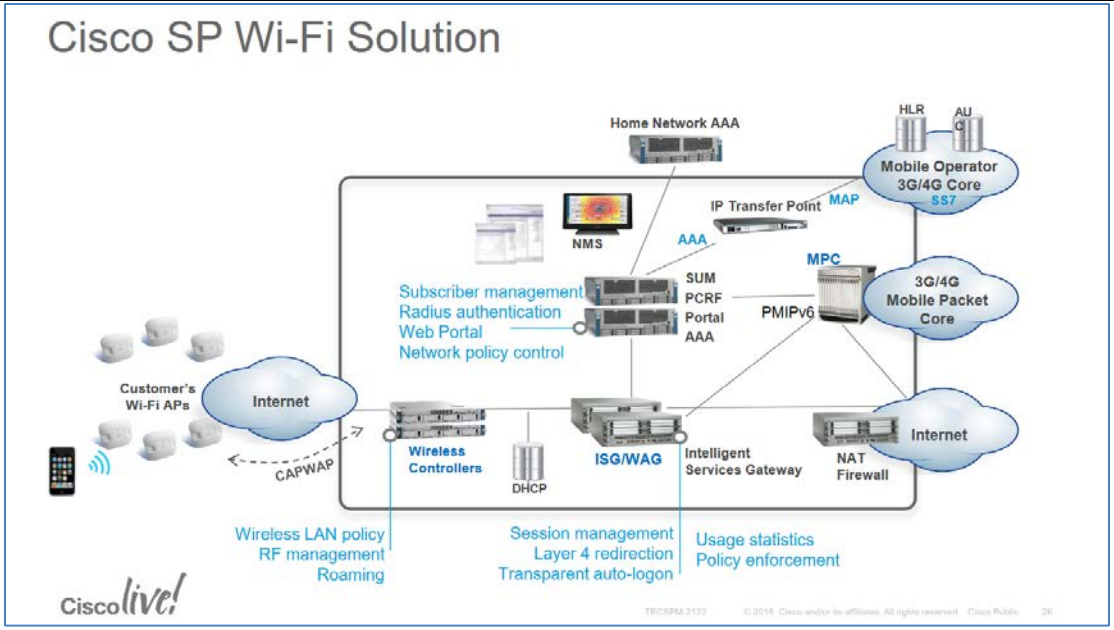
Cisco Unified Wireless Network Security Solutions

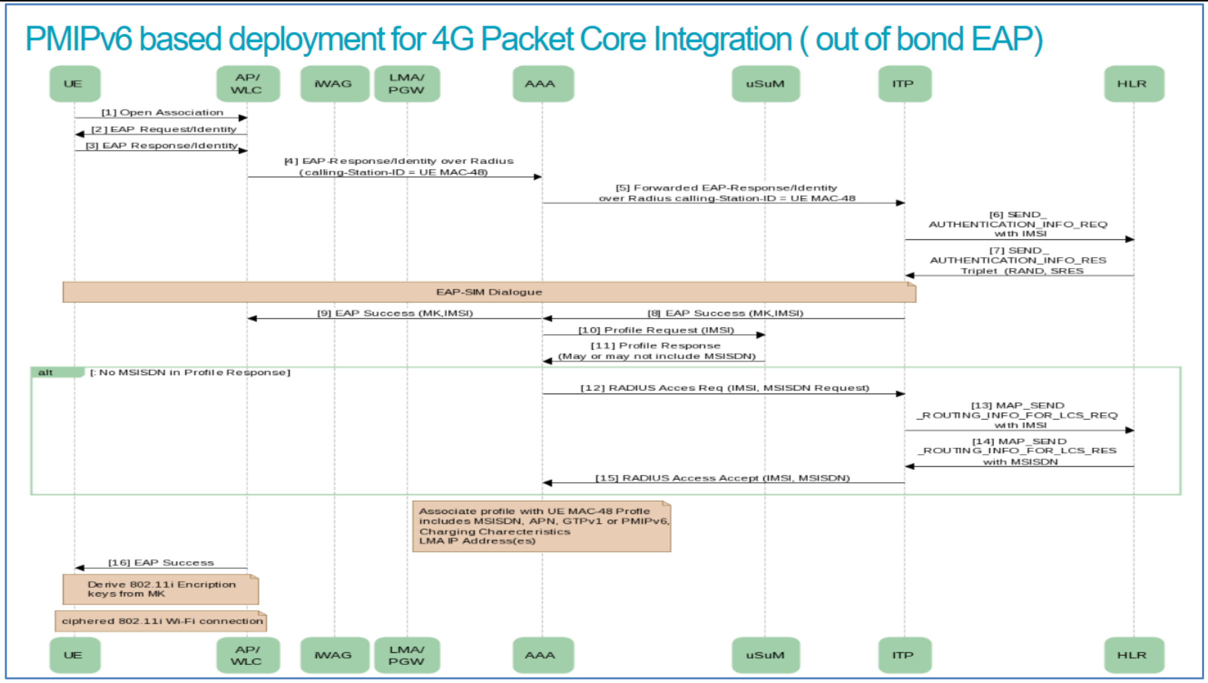
The Cisco Unified Wireless Network supports Layer 2 and Layer 3 security methods.

• Layer 2 security
• Layer 3 security (for WLAN) or Layer 3 security (for Guest LAN)

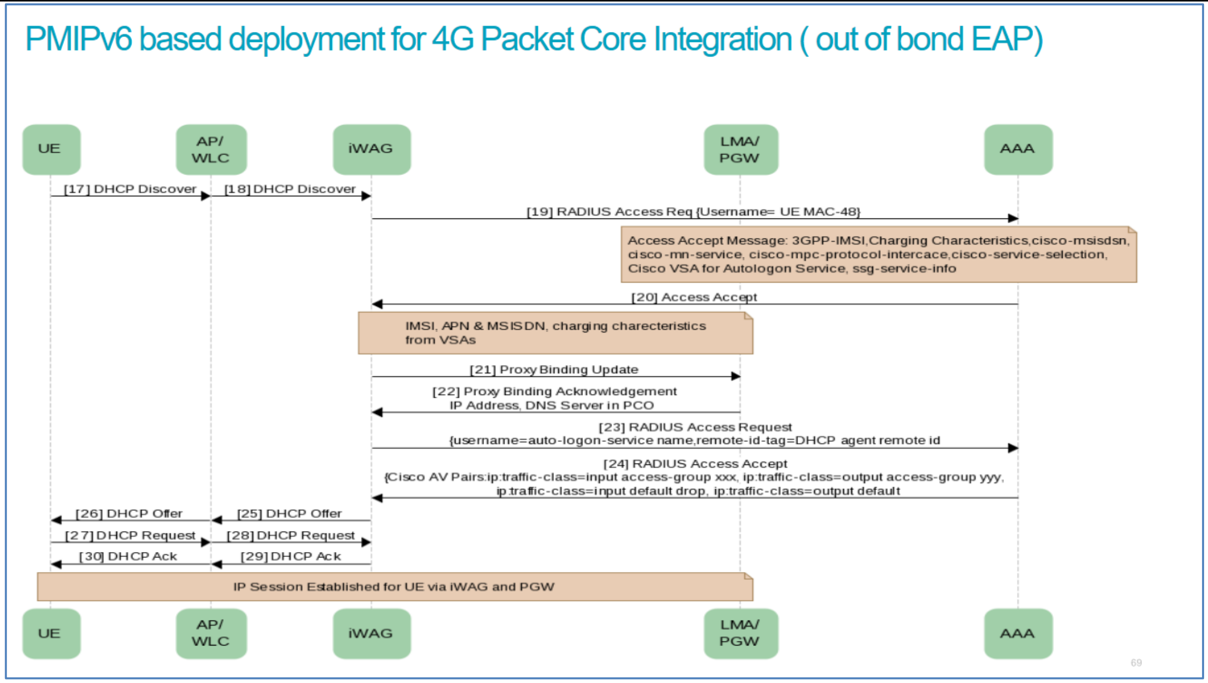
See, e.g., Wireless LAN Controller Layer 2 Layer 3 Security Compatibility Matrix, CISCO, https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106082-wlc-compatibility-matrix.html (last accessed June 18, 2021) (describing, based on a Cisco 4400/2100 Series WLC,</td>
</tr>
</table>

	various Layer 2 and Layer 3 (i.e., "higher than layer 2 monitoring entity") security methods supported on the Wireless LAN Controller).
CLAIM 6	
6[A] A system according to claim 5 wherein the ICME is a layer 2 monitoring entity and wherein the inter-technology change-off is between UMTS and WLAN and wherein a change-off is detected when an association occurs.	Cisco's SP Wi-Fi provides a system according to claim 5 wherein the ICME is a layer 2 monitoring entity and wherein the inter-technology change-off is between UMTS and WLAN and wherein a change-off is detected when an association occurs. Cisco SP Wi-Fi APs or WLCs (e.g., "the ICME") are connected to by user equipment (UE). The ICME detects the inter-technology change-off of the UE from a first access technology (e.g., 3G/4G) of the converged network to a second access technology (e.g., Wi-Fi) of the converged network and transmits a Dynamic Host Configuration Protocol (DHCP) message (e.g., "the ICME is a layer 2 monitoring entity and wherein the inter-technology change-off is between UMTS and WLAN and wherein a change-off is detected when an association occurs"). *See TECSPM* at 26, 68-69 (disclosing Cisco's UE to WLAN handover process in the Cisco SP Wi-Fi system).

	Cisco SP Wi-Fi Solution Home Network AAA HLR Mobile Operator 3G/4G Core SS7 IP Transfer Point MAP NMS AAA MPC Subscriber management Radius authentication Web Portal Network policy control SUM PCRF Portal AAA PMIPv6 3G/4G Mobile Packet Core Customer's Wi-Fi APs Internet CAPWAP Wireless Controllers DHCP ISG/WAG Intelligent Services Gateway NAT Firewall Internet Wireless LAN policy RF management Roaming Session management Layer 4 redirection Transparent auto-logon Usage statistics Policy enforcement Ciscolive! *Id*. at 26.


PMIPv6 based deployment for 4G Packet Core Integration (out of bond EAP)
UE
AP/ WLC
iWAG
LMA/ PGW
AAA
uSuM
ITP
HLR
[1] Open Association
[2] EAP Request/Identity
[3] EAP Response/Identity
[4] EAP-Response/Identity over Radius (calling-Station-ID = UE MAC-48)
[5] Forwarded EAP-Response/Identity over Radius calling-Station-ID = UE MAC-48
[6] SEND_ AUTHENTICATION_INFO_REQ with IMSI
[7] SEND_ AUTHENTICATION_INFO_RES Triplet (RAND, SRES
EAP-SIM Dialogue
[9] EAP Success (MK,IMSI)
[8] EAP Success (MK,IMSI)
[10] Profile Request (IMSI)
[11] Profile Response (May or may not include MSISDN)
alt
[: No MSISDN in Profile Response]
[12] RADIUS Acces Req (IMSI, MSISDN Request)
[13] MAP_SEND _ROUTING_INFO_FOR_LCS_REQ with IMSI
[14] MAP_SEND _ROUTING_INFO_FOR_LCS_RES with MSISDN
[15] RADIUS Access Accept (IMSI, MSISDN)
Associate profile with UE MAC-48 Profle includes MSISDN, APN, GTPv1 or PMIPv6, Charging Charecteristics LMA IP Address(es)
[16] EAP Success
Derive 802.11i Encription keys from MK
ciphered 802.11i Wi-Fi connection

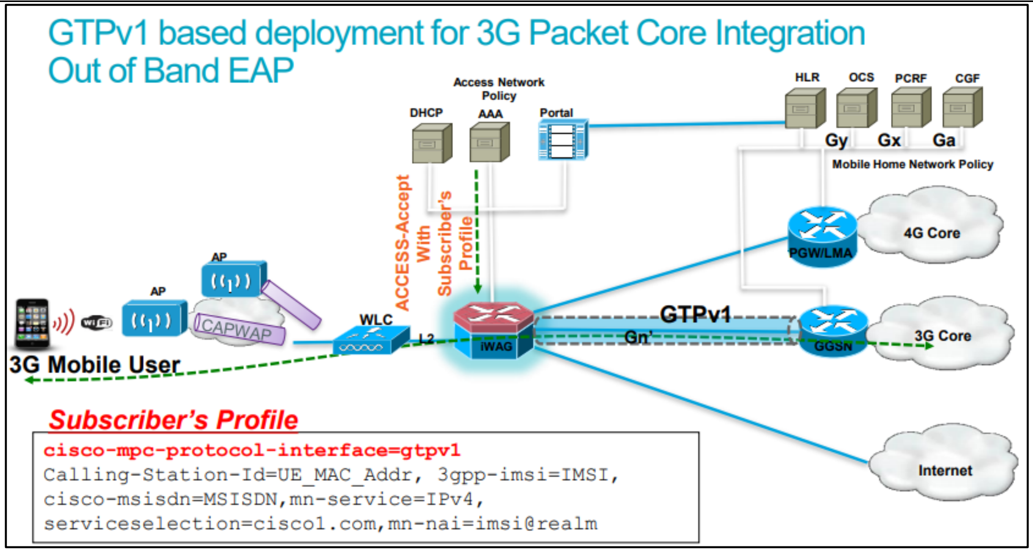
Id. at 68.

<table>
<tr>
<td></td>
<td>


Id. at 69.
</td>
</tr>
<tr>
<td colspan="2">CLAIM 7</td>
</tr>
<tr>
<td>7[A] A system according to claim 5 wherein the ICME is a layer 3 monitoring entity and wherein the inter-technology change-off is between UMTS and WLAN and wherein</td>
<td>Cisco’s SP Wi-Fi provides a system according to claim 5 wherein the ICME is a layer 3 monitoring entity and wherein the inter-technology change-off is between UMTS and WLAN and wherein the change-off is detected on an occurrence of a change in an IP address allocated to the multimodal device, receipt of a message from the multimodal mobile device, receipt of a DHCP message, or any other mechanism from the network or device to initiate a layer 3 handoff or change-off.

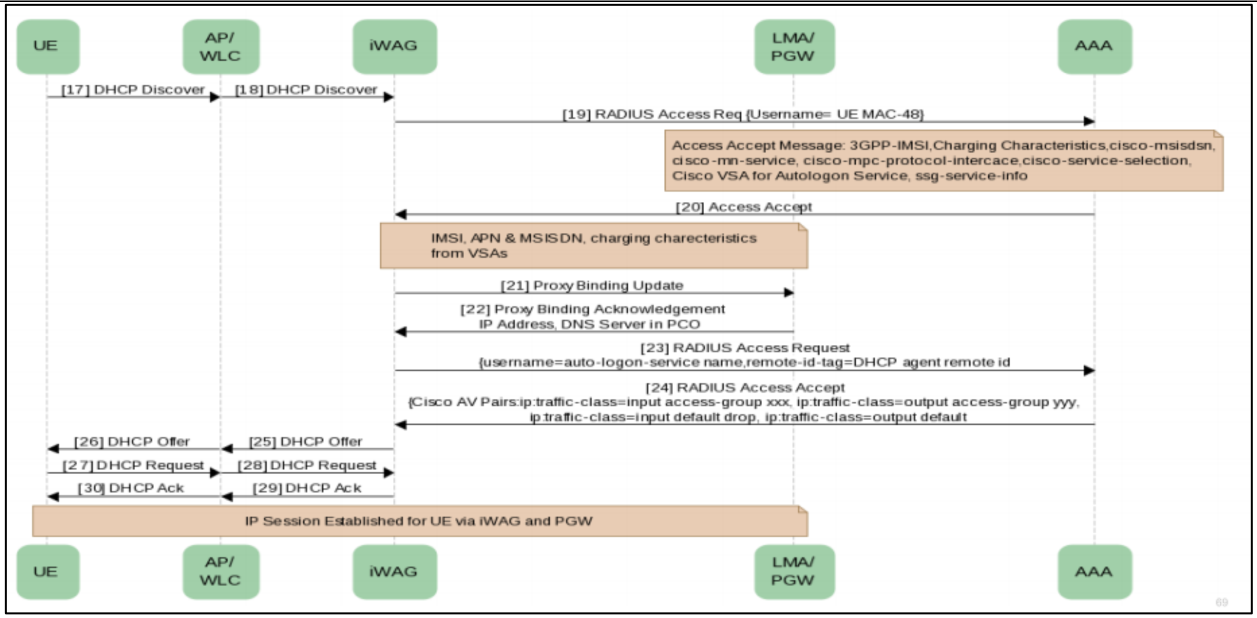
Cisco’s SP Wi-Fi supports ICME (i.e., handover) between, as one non-limiting example, 3G (i.e., UMTS) and Wi-Fi (i.e., WLAN) access networks.</td>
</tr>
</table>

<table>
<tr>
<td>the change-off is detected on an occurrence of a change in an IP address allocated to the multimodal device, receipt of a message from the multimodal mobile device, receipt of a DHCP message, or any other mechanism from the network or device to initiate a layer 3 handoff or change-off.</td>
<td>



See TECSPM at 62.

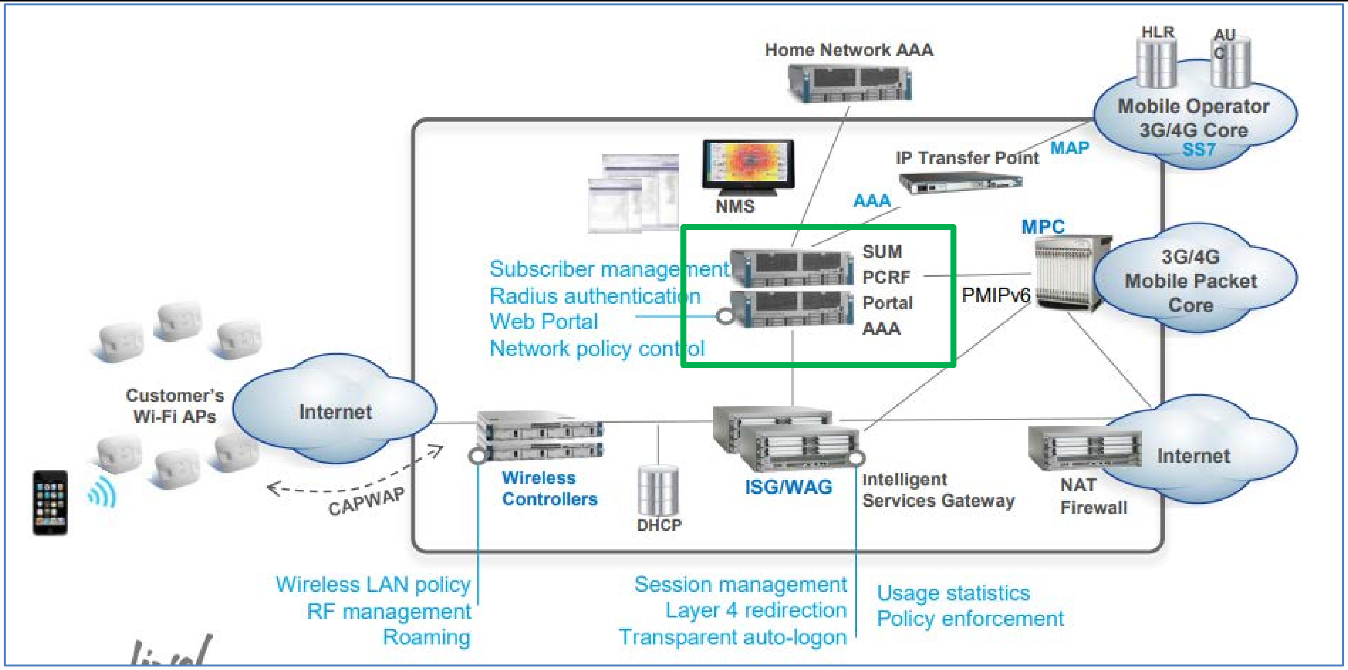
The WLC (e.g., "the ICME is a layer 3 monitoring entity") detects the inter-technology handover of the UE via a DHCP message when the UE is associated with the Wi-Fi access network (e.g., "inter-technology change-off is between UMTS and WLAN and wherein the change-off is detected on an occurrence of a change in an IP address allocated to the multimodal device, receipt of a message from the multimodal mobile device, receipt of a DHCP message, or any other mechanism from the network or device to initiate a layer 3 handoff or change-off"). *Id.* at 69.
</td>
</tr>
</table>

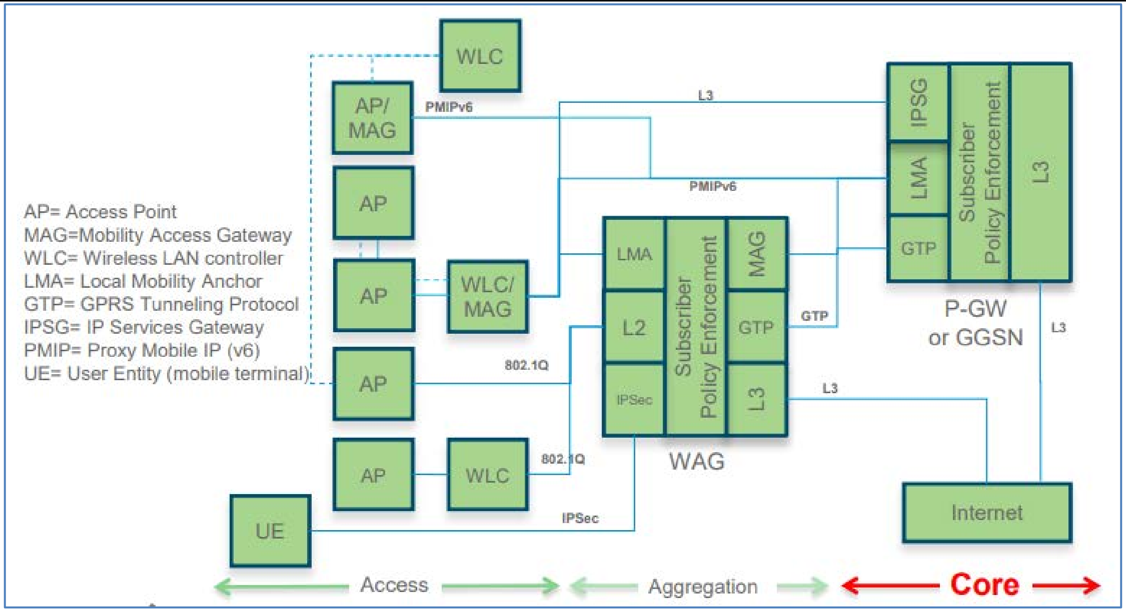


Id. at 69.

CLAIM 8

8[A] A system according to claim 1 wherein said appropriate policy is a combination of said user policy and said access technology policy, and wherein portions of said appropriate policy are distributed to	Cisco's SP Wi-Fi provides a system according to claim 1 wherein said appropriate policy is a combination of said user policy and said access technology policy, and wherein portions of said appropriate policy are distributed to each PEF of said at least one PEF. User-enforced policies (i.e., appropriate policy) are the combination of applicable network policies (i.e., said access technology policy) and subscriber enforcement policies (i.e., user policy).

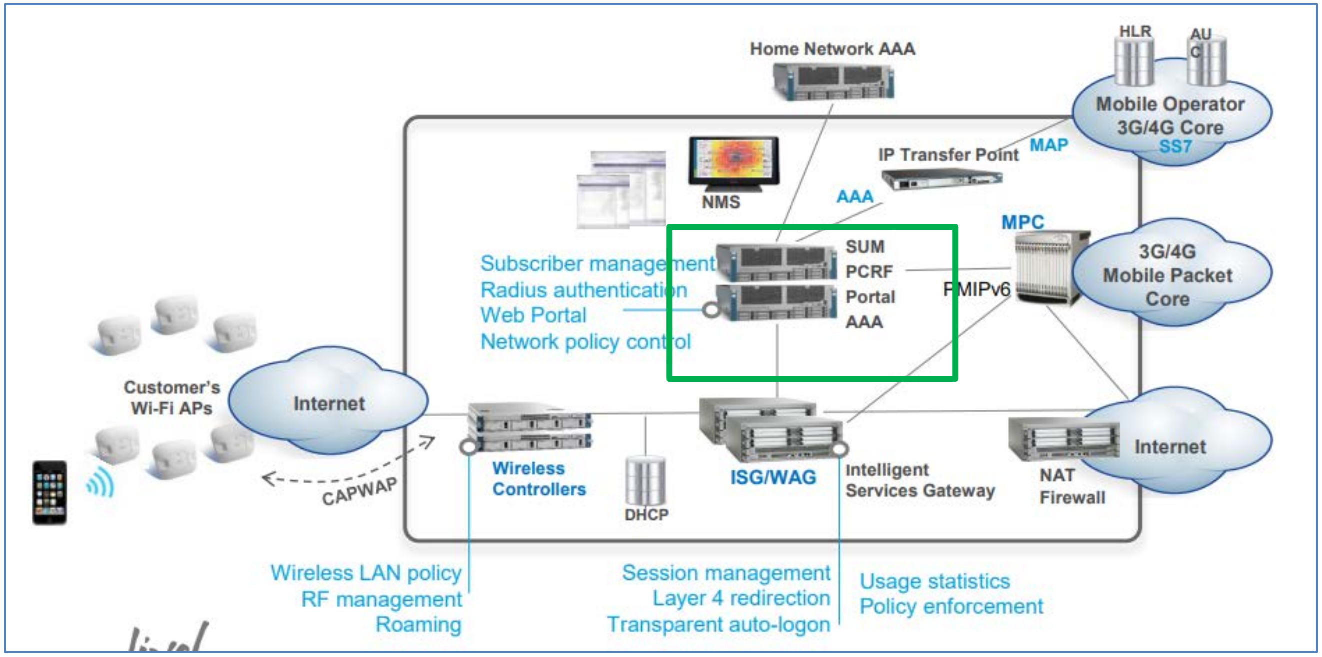
each PEF of said at least one PEF.	 *See TECSPM* at 26. Further, Cisco's SP Wi-Fi (via, e.g., the WAG) applies a subscriber enforcement policy based on the subscriber's profile.

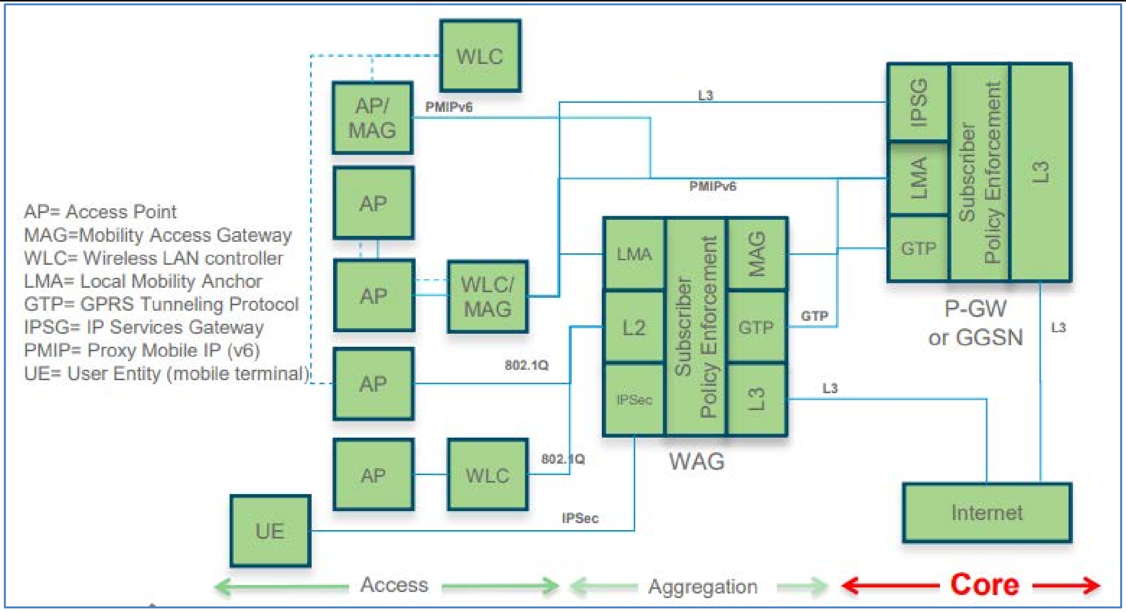
	 *Id.* at 34. Cisco ISG/WAG provide policy management services for different access networks as well as policy enforcement functions. *See SP WiFi: Deploying Access for 3G and 4G Mobile Networks*, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 27 (last accessed June 18, 2021) (describing ISG and IOS relationship with regards to policy management).

Id. at 27.

The ISG/WAG act as a policy manager as well as the policy enforcement point (PEF). The Policy management function within the ISG/WAG decides the policies for user access. For example, the policy manager (i.e., ISG/WAG) decides whether to create a dedicated (complete) or a minimal (lite) session. *See Intelligent Services Gateway Configuration Guide Cisco IOS XE Release 3S*, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-3s/isg-xe-3s-book/isg-wlkby-supp.html, at 27 (last accessed June 18, 2021).

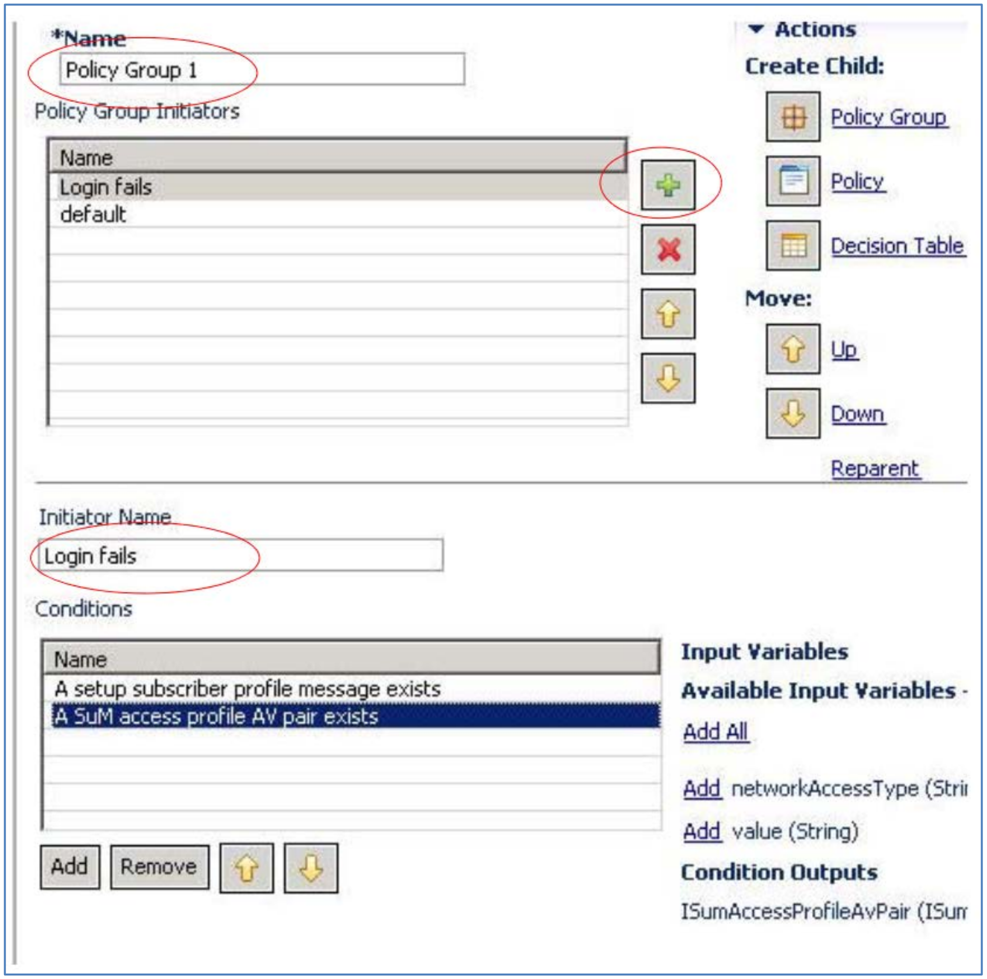
	Dedicated Sessions A dedicated or regular session is a full-fledged Intelligent Services Gateway (ISG) subscriber session. All subscriber sessions that are authenticated cause the creation of dedicated sessions on ISG. The policy manager of ISG decides whether to create a complete session context (a dedicated session) or a minimal session context (a lite session). Note: ISG provides high availability support for converted (lite to dedicated) unclassified and DHCPv4 sessions. **Supported Triggers** Walk-by sessions can be created through any of the following session initiators: • Packet trigger: Here the session creation is triggered by a subscriber's IP packet having an unclassified IP address or MAC address. • RADIUS proxy: This trigger is commonly used in PWLAN deployments where ISG acts as a RADIUS proxy. Here, the session creation is triggered by the subscriber's RADIUS packets. • DHCP: This trigger is another SIP used in a few PWLAN deployments. Here, the session creation is triggered by the subscriber's DHCP control packets. • EoGRE walkby: When ISG is configured for EoGRE, DHCP control packets and unclassified MAC packets on the EoGRE interface trigger session creation on ISG. *Id*. at 27. Within the ISG/WAG, the policy manager distributes the policies to the policy enforcement point (PEF) to enforce them for a user. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 199 (last accessed June 18, 2021). A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however. Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource. *Id*. at 199.

CLAIM 9	
9[A] A system according to claim 8 wherein said combination of said user policy and said access technology policy is a sum of said user policy plus said access technology policy.	Cisco's SP Wi-Fi provides a system according to claim 8 wherein said combination of said user policy and said access technology policy is a sum of said user policy plus said access technology policy. Cisco's WAG applies a user policy which is the combination of an applicable network policy and a subscriber enforcement policy (e.g., "wherein said combination of said user policy and said access technology policy is a sum of said user policy plus said access technology policy").  *See TECSPM* at 26.

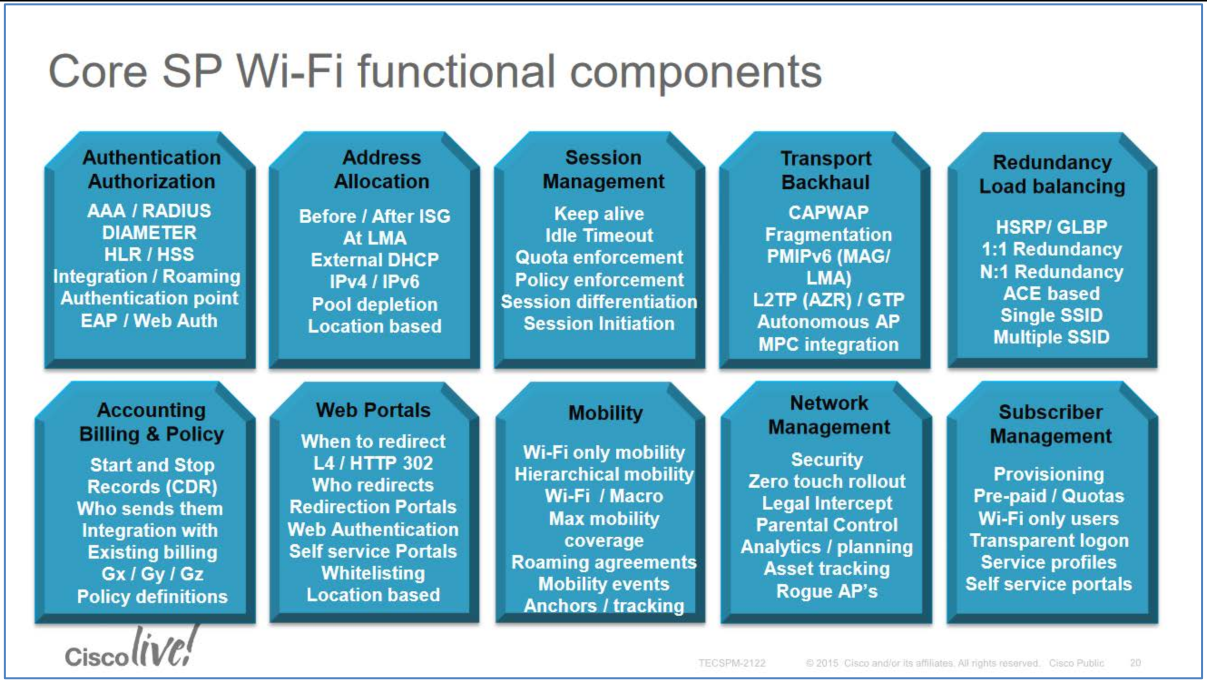
	WLC AP/ MAG PMIPv6 L3 IPSG LMA GTP Subscriber Policy Enforcement L3 PMIPv6 AP= Access Point MAG=Mobility Access Gateway WLC= Wireless LAN controller LMA= Local Mobility Anchor GTP= GPRS Tunneling Protocol IPSG= IP Services Gateway PMIP= Proxy Mobile IP (v6) UE= User Entity (mobile terminal) AP AP WLC/ MAG LMA Subscriber Policy Enforcement MAG L2 GTP GTP P-GW or GGSN L3 802.1Q AP IPSec L3 L3 WAG AP WLC 802.1Q UE IPSec Internet Access Aggregation Core *Id.* at 34.

	Cisco Policy Suite adapts to a variety of sources for subscriber data. Possible subscriber profile repositories (SPR) that may be available to you are: • Cisco Control Center interface component of CPS • Cisco's Unified Subscriber Manager (Cisco Unified SuM) component of CPS • Cisco's AAA server component of CPS • LDAP • AAA This flexibility lets you include either an external subscriber management system in your Cisco Policy Builder architecture or the internal, integrated Cisco Unified SuM. Subscriber management schemes vary and are particular to an individual network. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 209 (last accessed June 18, 2021).

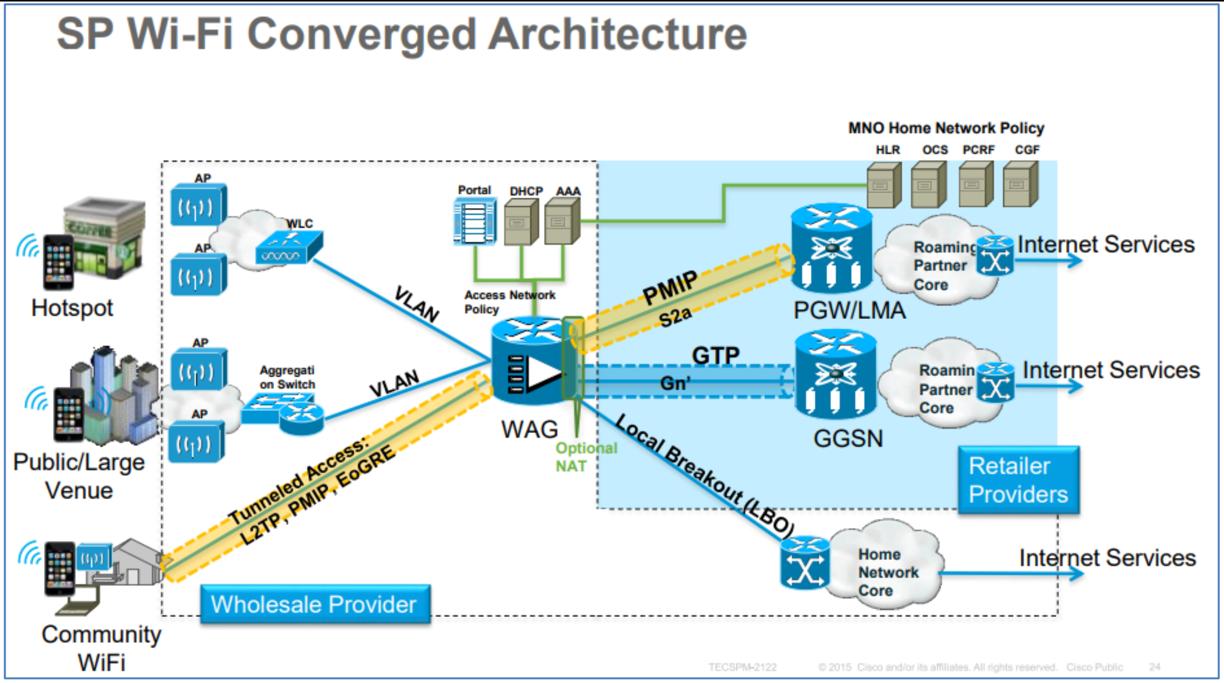
	The Initial Blueprint executes the following policy flow. • Pre-Session Policies. These are policies not associated with a subscriber session. They are defined in the "Pre-session policies". • Load Session. Upon receiving a policy message, the load session policies attempt to load the session using keys that are retrieved from the input message. • Stop Session. Upon loading a session, the session can be stopped if "Stop session" criteria is fulfilled (for example, a RADIUS stop message can be a stop session criteria). • Start Session. If a session does not exist, then a new session can be started if the "Start session" criteria is fulfilled (for example, a RADIUS start message can be a start session criteria). • Active Session Policies. If a session is active then the active session policies are initiated. The active session policies are executed in the following order: – Map session data from input. This maps data from the input record to the network session (for example, mapping the user ID from a RADIUS record). *Id.* at 213. The Network Session node is always part of the Initial Blueprint. This node describes the data you want to capture for each subscriber's session. The Initial Blueprint defines the set of attributes used in the NetworkSession that are common across all network sessions. These attributes can be: • macAddress—the MAC address of the device connected to the network • userId—the user ID of the subscriber connected to the network • framedIp—the framed IP of the subscriber's network connection • circuitId—the circuit ID of the subscriber's network connection • avps—the list of AVPs (attribute value pairs) associated with the subscriber's network session • devices—the list of network devices associated with the subscriber's network session *Id.* at 228.

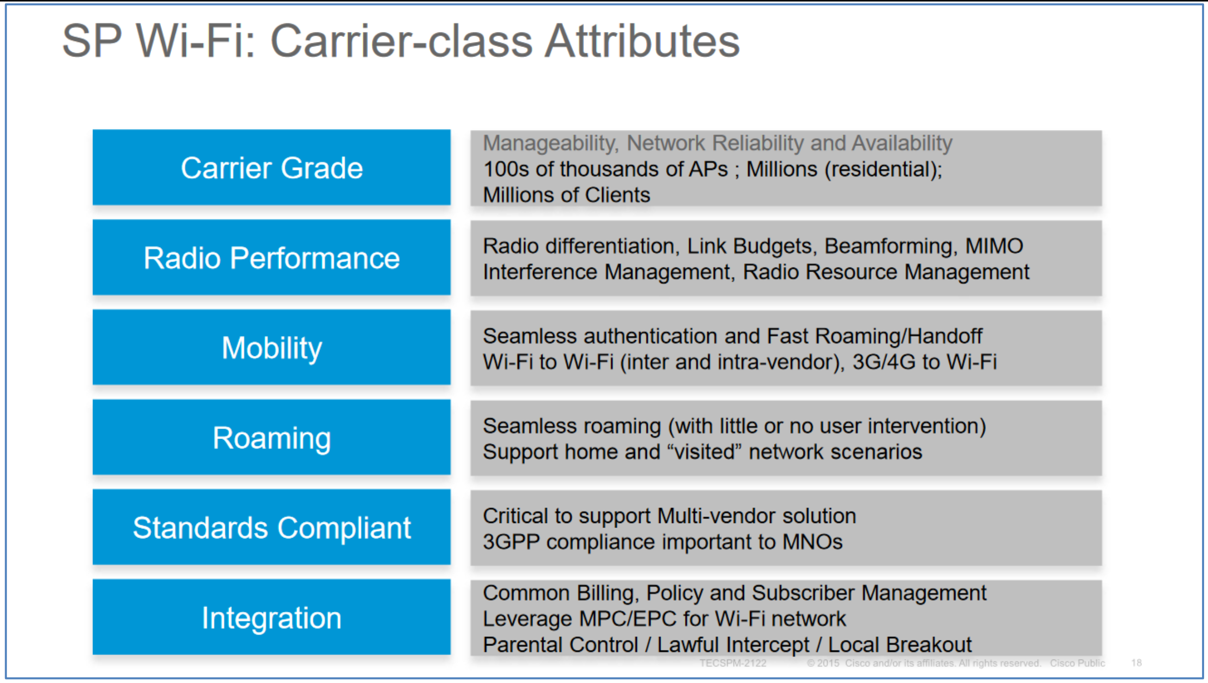
	 *Id*. at 251 (portraying configuration of user policies combining network access policies and subscriber policies).

CLAIM 10	
10[Pre.] A method for network access security policy management of multimodal access to a converged network, the method comprising:	To any extent the preamble is limiting, Cisco's SP Wi-Fi provides a method for network access security policy management of multimodal access to a converged network. Cisco's SP Wi-Fi is used to provide a method for network access security policy management of multimodal access to a converged network, comprising various hardware elements including, but not limited to, Access Points (APs), Wireless Controllers (WLCs), Wireless Access Gateways (WAGs), Packet Gateways (PGWs), PCRFs (Policy and Charging Rule Functions), and PCEFs (Policy and Charging Enforcement Functions).  *See TECSPM* at 19.

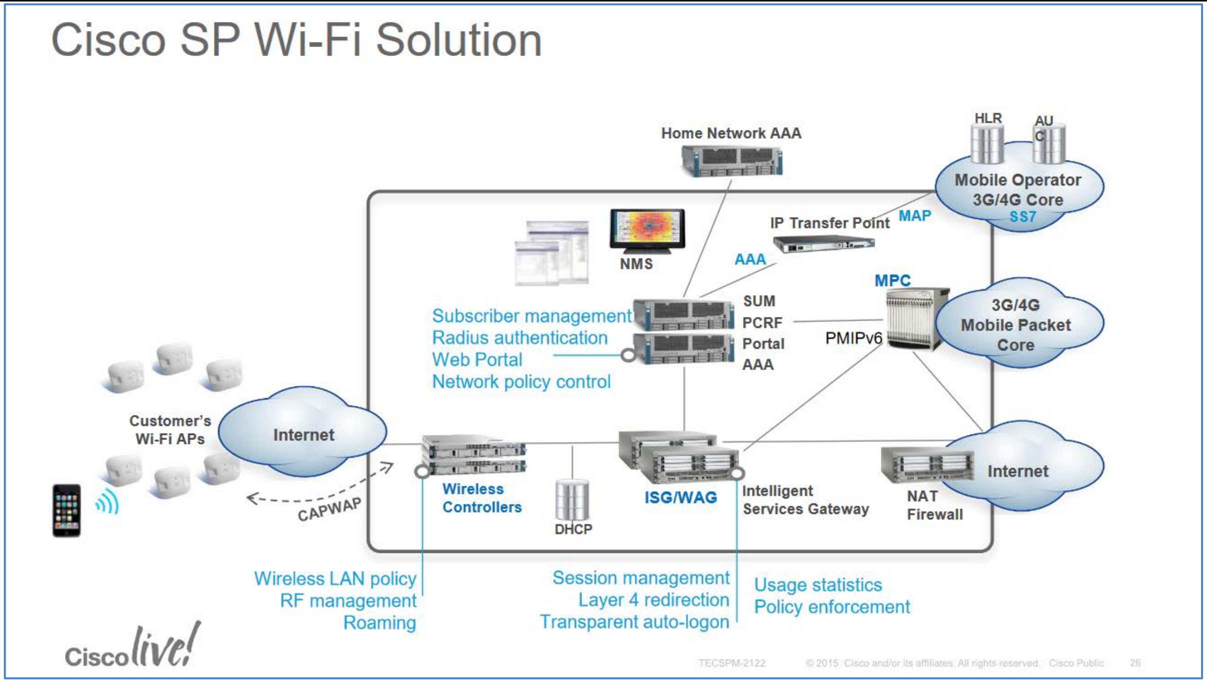

Core SP Wi-Fi functional components
Authentication Authorization
AAA / RADIUS
DIAMETER
HLR / HSS
Integration / Roaming
Authentication point
EAP / Web Auth
Address Allocation
Before / After ISG
At LMA
External DHCP
IPv4 / IPv6
Pool depletion
Location based
Session Management
Keep alive
Idle Timeout
Quota enforcement
Policy enforcement
Session differentiation
Session Initiation
Transport Backhaul
CAPWAP
Fragmentation
PMIPv6 (MAG/ LMA)
L2TP (AZR) / GTP
Autonomous AP
MPC integration
Redundancy Load balancing
HSRP/ GLBP
1:1 Redundancy
N:1 Redundancy
ACE based
Single SSID
Multiple SSID
Accounting Billing & Policy
Start and Stop Records (CDR)
Who sends them
Integration with Existing billing
Gx / Gy / Gz
Policy definitions
Web Portals
When to redirect
L4 / HTTP 302
Who redirects
Redirection Portals
Web Authentication
Self service Portals
Whitelisting
Location based
Mobility
Wi-Fi only mobility
Hierarchical mobility
Wi-Fi / Macro
Max mobility coverage
Roaming agreements
Mobility events
Anchors / tracking
Network Management
Security
Zero touch rollout
Legal Intercept
Parental Control
Analytics / planning
Asset tracking
Rogue AP's
Subscriber Management
Provisioning
Pre-paid / Quotas
Wi-Fi only users
Transparent logon
Service profiles
Self service portals
Cisco live!
TECSPM-2122
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public
20

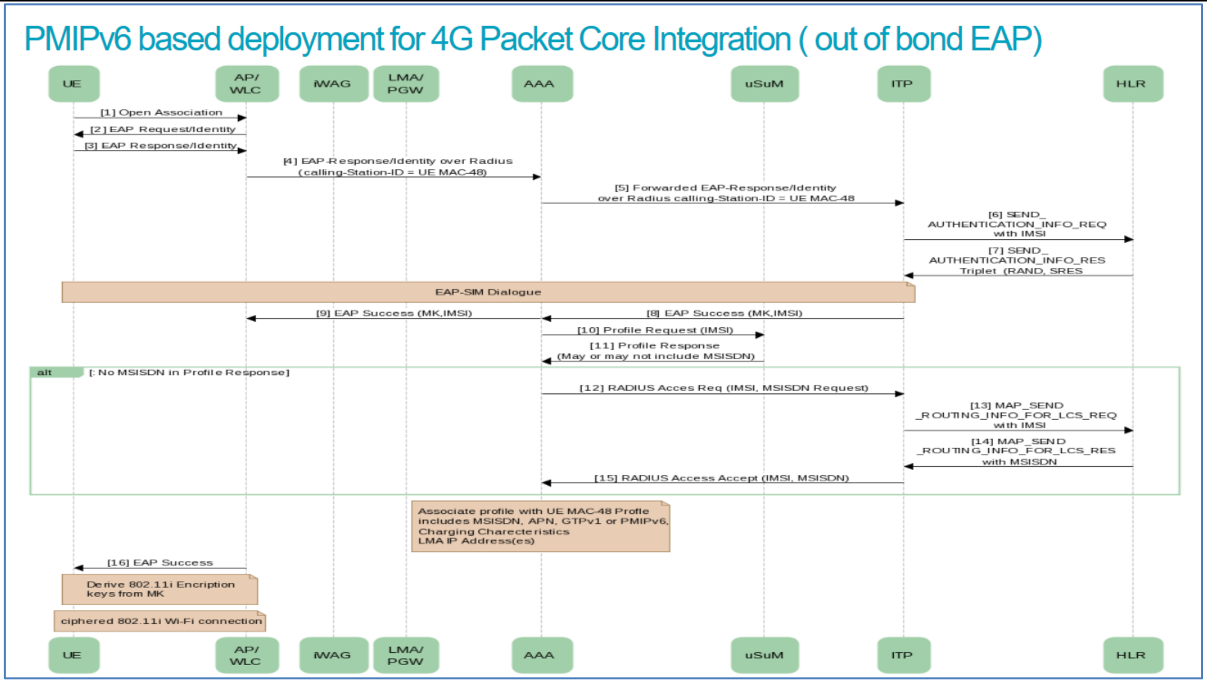
Id. at 20.

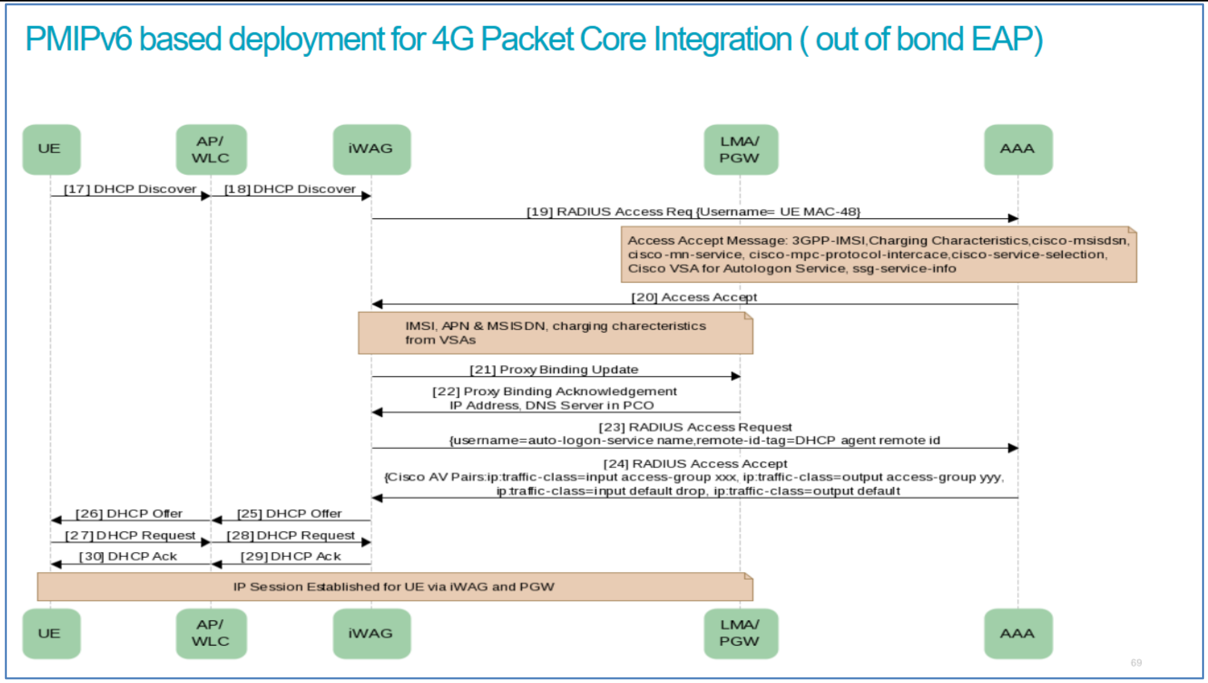
	 *Id*. at 24. Cisco's SP Wi-Fi provides seamless and efficient handoff between access technologies (e.g., 3G/4G to Wi-Fi) as well as offering policy and subscriber management features.



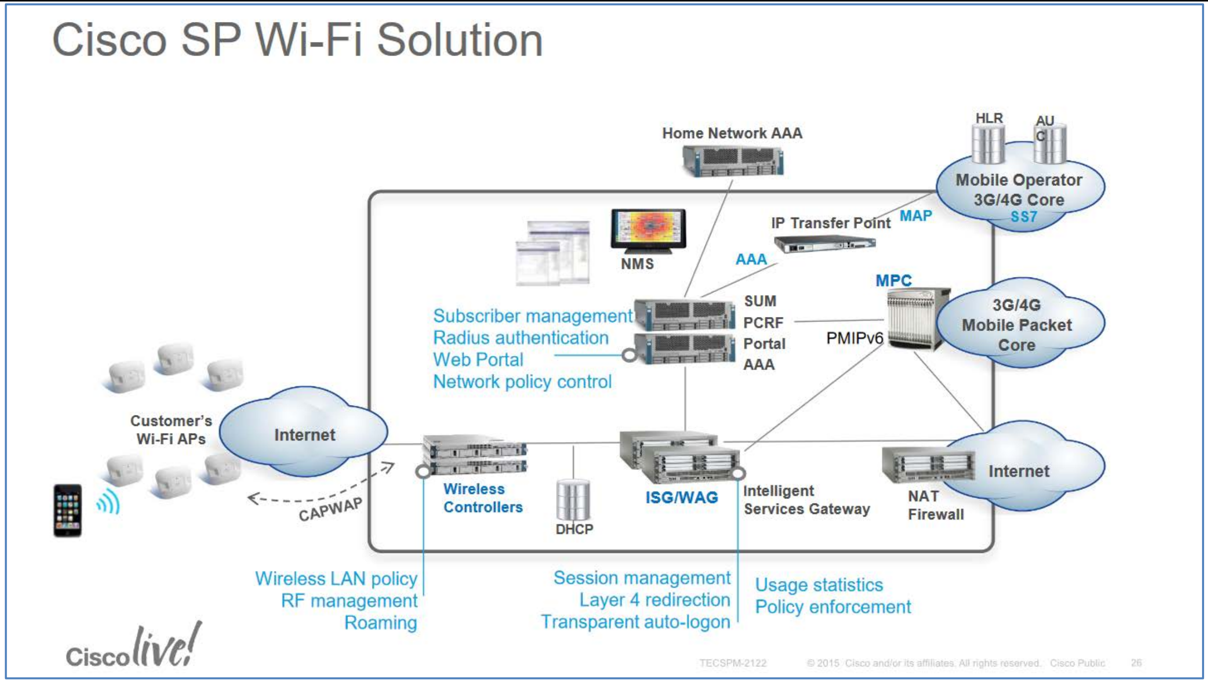
	Id. at 18.
10[A] detecting at an inter-technology change-off monitoring entity (ICME) occurrence of an inter-technology change-off of a multimodal device from a first access technology of the converged network to a second	Cisco's SP Wi-Fi method detects at an inter-technology change-off monitoring entity (ICME) the occurrence of an inter-technology change-off of a multimodal device from a first access technology of the converged network to a second access technology of the converged network. Cisco's SP Wi-Fi APs or WLCs (e.g., "an inter-technology change-off monitoring entity (ICME)") are connected to by user equipment (UE). The ICME detects the inter-technology change-off of the UE (e.g., "a multimodal device") from a first access technology (e.g., 3G/4G) of the converged network to a second access technology (e.g., Wi-Fi) of the converged network and transmits a Dynamic Host Configuration Protocol (DHCP) message (e.g., an "inter-technology change-off message"). *See TECSPM* at 26, 68-69 (disclosing Cisco's UE to WLAN handover (e.g., "inter-technology change-off of a multimodal device from a first access technology of the converged network to a second access technology of the converged network") process in the Cisco SP Wi-Fi system).

access technology of the converged network;	 *Id*. at 26.

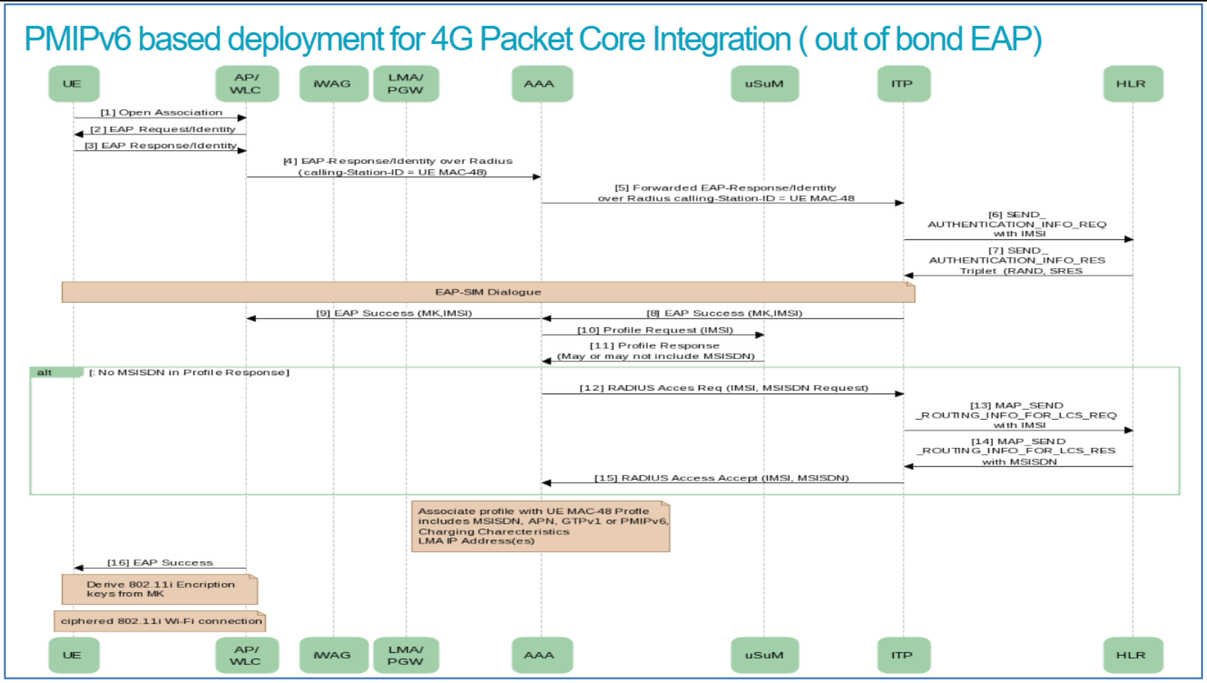
	PMIPv6 based deployment for 4G Packet Core Integration (out of bond EAP) UE AP/ WLC iWAG LMA/ PGW AAA uSuM ITP HLR [1] Open Association [2] EAP Request/Identity [3] EAP Response/Identity [4] EAP-Response/Identity over Radius (calling-Station-ID = UE MAC-48) [5] Forwarded EAP-Response/Identity over Radius calling-Station-ID = UE MAC-48 [6] SEND_ AUTHENTICATION_INFO_REQ with IMSI [7] SEND_ AUTHENTICATION_INFO_RES Triplet (RAND, SRES EAP-SIM Dialogue [9] EAP Success (MK,IMSI) [8] EAP Success (MK,IMSI) [10] Profile Request (IMSI) [11] Profile Response (May or may not include MSISDN) alt [: No MSISDN in Profile Response] [12] RADIUS Acces Req (IMSI, MSISDN Request) [13] MAP_SEND _ROUTING_INFO_FOR_LCS_REQ with IMSI [14] MAP_SEND _ROUTING_INFO_FOR_LCS_RES with MSISDN [15] RADIUS Access Accept (IMSI, MSISDN) Associate profile with UE MAC-48 Profle includes MSISDN, APN, GTPv1 or PMIPv6, Charging Charecteristics LMA IP Address(es) [16] EAP Success Derive 802.11i Encription keys from MK ciphered 802.11i Wi-Fi connection *Id*. at 68.

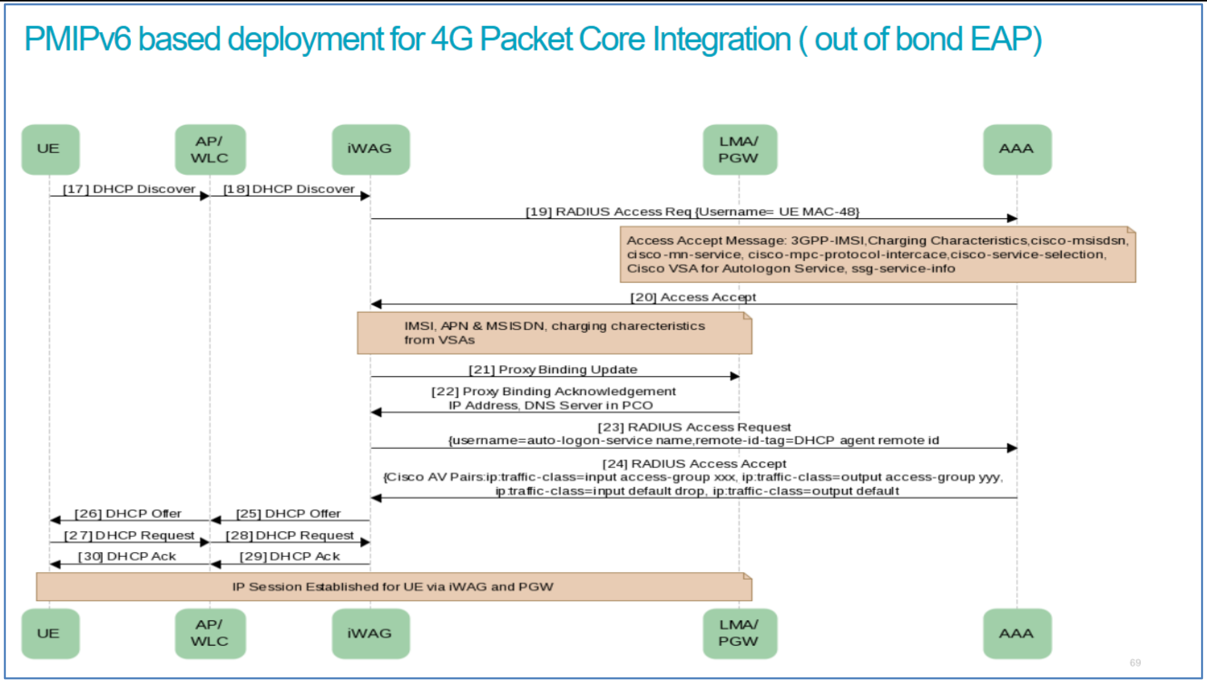
<table>
<tr>
<td></td>
<td>


Id. at 69.
</td>
</tr>
<tr>
<td>10[B] transmitting an inter-technology change-off message from said inter-technology change-off monitoring entity (ICME) to a policy manager;</td>
<td>Cisco’s SP Wi-Fi APs or WLCs (e.g., “an inter-technology change-off monitoring entity (ICME)”) are connected to by user equipment (UE). The ICME transmits a Dynamic Host Configuration Protocol (DHCP) message to an iWAG (e.g., “transmitting an inter-technology change-off message from said inter-technology change-off monitoring entity (ICME) to a policy manager”). See TECSPM at 26, 68-69 (disclosing Cisco’s UE to WLAN handover process in the Cisco SP Wi-Fi system).</td>
</tr>
</table>


Cisco SP Wi-Fi Solution
Home Network AAA
HLR
AU
C
Mobile Operator 3G/4G Core
SS7
MAP
IP Transfer Point
AAA
NMS
MPC
SUM
PCRF
Portal
AAA
PMIPv6
3G/4G Mobile Packet Core
Subscriber management
Radius authentication
Web Portal
Network policy control
Customer's Wi-Fi APs
Internet
CAPWAP
Wireless Controllers
DHCP
ISG/WAG
Intelligent Services Gateway
NAT Firewall
Internet
Wireless LAN policy
RF management
Roaming
Session management
Layer 4 redirection
Transparent auto-logon
Usage statistics
Policy enforcement
Cisco live!
TECSPM-2122
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public
26

Id. at 26.

	 PMIPv6 based deployment for 4G Packet Core Integration (out of bond EAP) UE AP/ WLC iWAG LMA/ PGW AAA uSuM ITP HLR [1] Open Association [2] EAP Request/Identity [3] EAP Response/Identity [4] EAP-Response/Identity over Radius (calling-Station-ID = UE MAC-48) [5] Forwarded EAP-Response/Identity over Radius calling-Station-ID = UE MAC-48 [6] SEND_ AUTHENTICATION_INFO_REQ with IMSI [7] SEND_ AUTHENTICATION_INFO_RES Triplet (RAND, SRES EAP-SIM Dialogue [9] EAP Success (MK,IMSI) [8] EAP Success (MK,IMSI) [10] Profile Request (IMSI) [11] Profile Response (May or may not include MSISDN) alt [: No MSISDN in Profile Response] [12] RADIUS Acces Req (IMSI, MSISDN Request) [13] MAP_SEND _ROUTING_INFO_FOR_LCS_REQ with IMSI [14] MAP_SEND _ROUTING_INFO_FOR_LCS_RES with MSISDN [15] RADIUS Access Accept (IMSI, MSISDN) Associate profile with UE MAC-48 Profile includes MSISDN, APN, GTPv1 or PMIPv6, Charging Charecteristics LMA IP Address(es) [16] EAP Success Derive 802.11i Encription keys from MK ciphered 802.11i Wi-Fi connection *Id*. at 68.

<table>
<tr>
<td></td>
<td>


Id. at 69.
</td>
</tr>
<tr>
<td>10[C] searching a policy database by said policy manager for an access technology policy corresponding to said second access technology;</td>
<td>Cisco’s SP Wi-Fi method searches a policy database by said policy manager for an access technology policy corresponding to said second access technology.

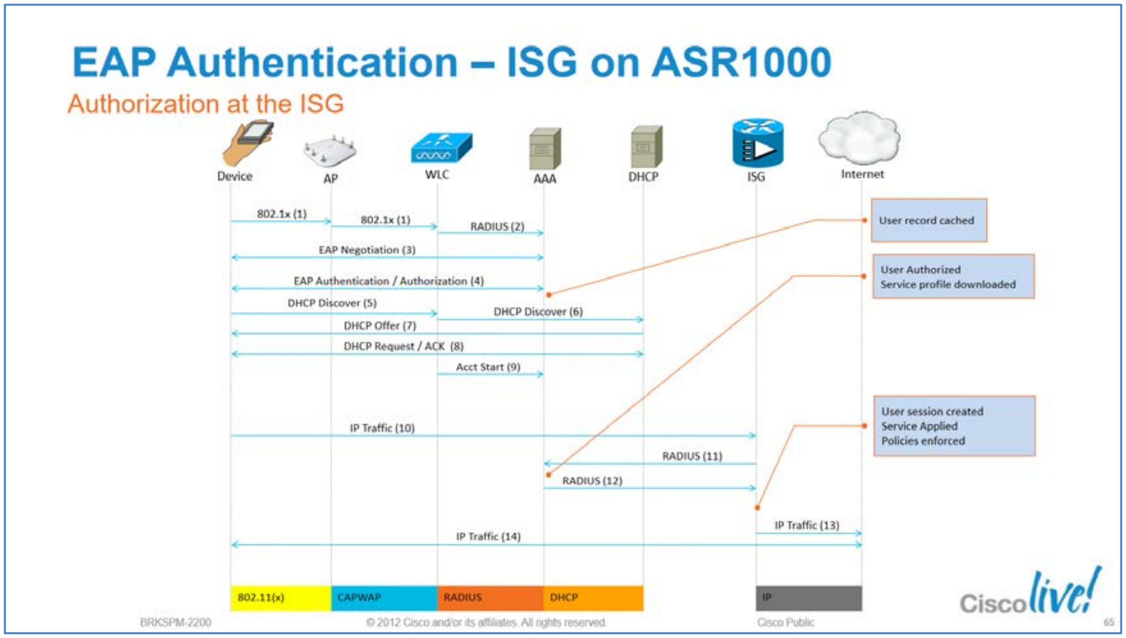
Cisco’s SP Wi-Fi utilizes one or more Intelligent Wireless Access Gateways (iWAGs). The iWaG(s) are aware of ISG subscriber awareness through a connection to AAA servers or PCRF (e.g., “searching a policy database by said policy manager for an access technology policy corresponding to said second access technology”), to enable 3G/4G offloading to Wi-Fi.</td>
</tr>
</table>

	Service providers use a combination of WiFi and mobility offerings to offload their mobility networks in the area of high-concentration service usage. This led to the evolution of the Intelligent Wireless Access Gateway (iWAG). The iWAG provides a WiFi offload option to 4G and 3G service providers by enabling a single-box solution that provides the combined functionality of Proxy Mobile IPv6 (PMIPv6) and GPRS Tunneling Protocol (GTP) on the Cisco Intelligent Services Gateway (Cisco ISG) framework. This document provides information about the iWAG and how to configure it, and contains the following sections: *See Intelligent Wireless Access Gateway Configuration Guide*, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iwag/configuration/xe-3s/IWAG_Config_Guide_BookMap/iwag-overview.html (last accessed June 18, 2021).
10[D] determining at the policy manager appropriate security policies to be enforced;	Cisco's Policy Enforcement Points (PEPs per Cisco documentation; PEFs per the '106 patent) are a component of policy-based management implementable by Cisco's ISGs or iWAGs.

	At install time, you need to determine what policy enforcement points your installation use and what features you need to install. PEPS might be: • Cisco ISG pool • Cisco ASR 5K • Cisco ASR9K • MAG • IWAG • Cisco WLC • SCE Device Pool • RADIUS AAA server or device pool • Procera • Allot • PDSN • PCEF Consult your Cisco technical representative for configuring a custom site. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 200 (last accessed June 18, 2021). Cisco's PEPs and PDPs, as one non-limiting example, perform "the job of deciding whether or not to authorize the user based on the description of the user's attributes" (e.g., "determin[e] at the policy manager appropriate security policies to be enforced").

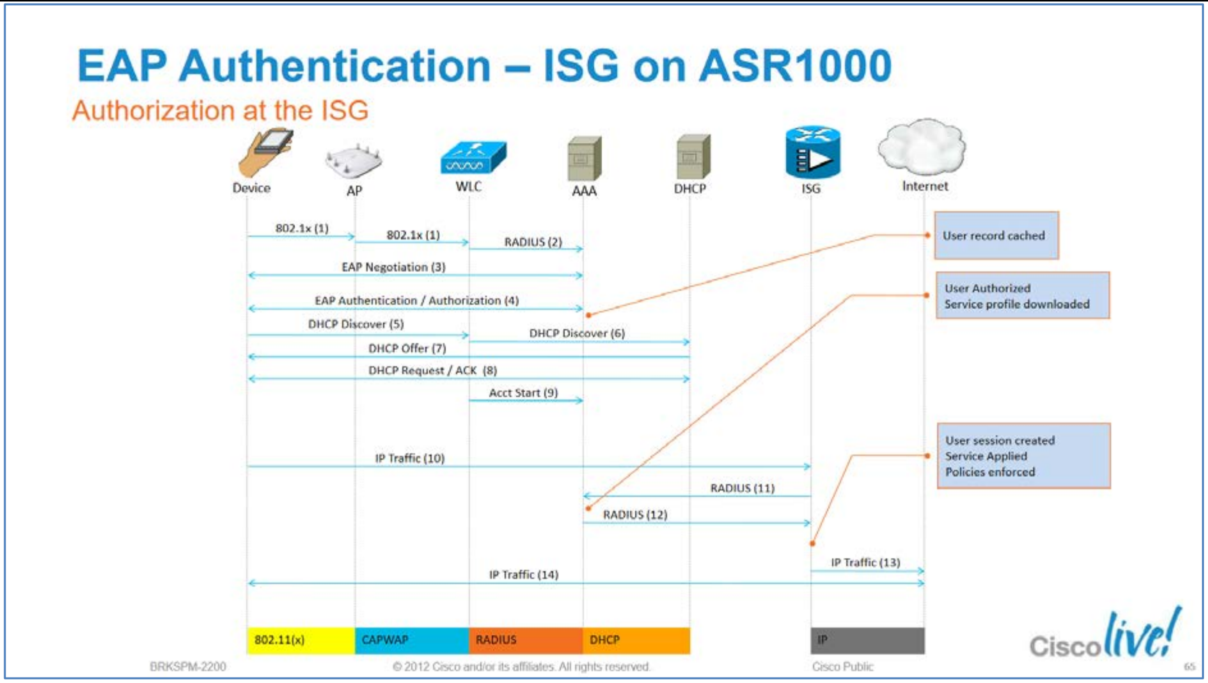
> A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however.
>
> Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource.

Id. at 199.



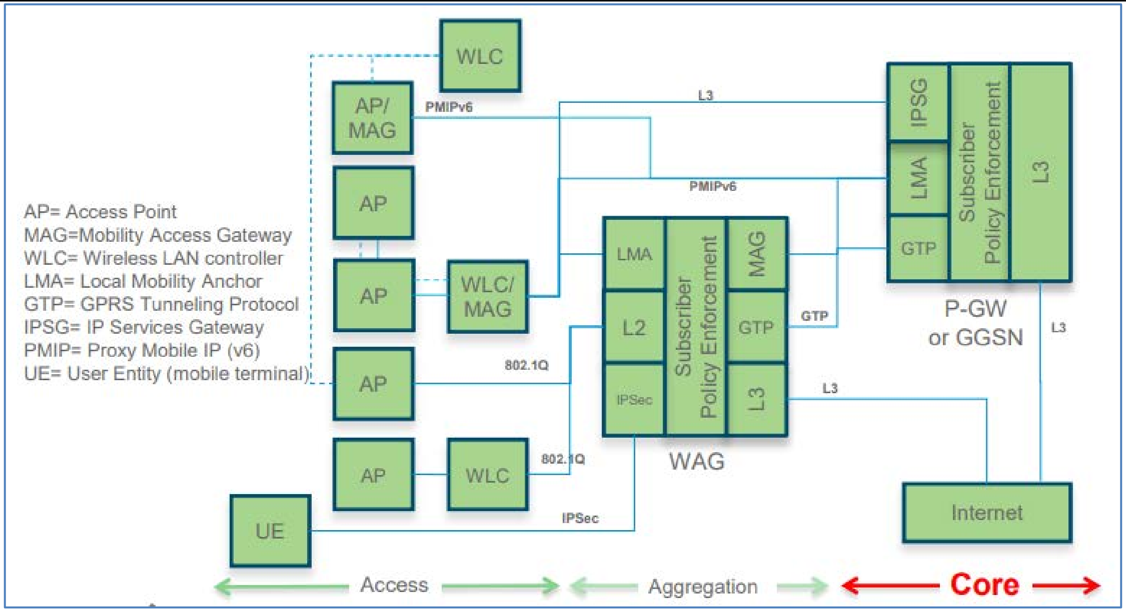
See SP WiFi: Deploying Access for 3G and 4G Mobile Networks, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 65 (last accessed June 18, 2021) (describing ISG authorization flow).

10[E] distributing from said policy manager to at least one policy enforcement point (PEF) said appropriate security policies; and	Cisco's SP Wi-Fi method distributes from said policy manager to at least one policy enforcement point (PEF) said appropriate security policies. Cisco's Policy Enforcement Points (PEPs per Cisco documentation; PEFs per the '106 patent) are a component of policy-based management (e.g., "distributing from said policy manager to at least one policy enforcement point (PEF) said appropriate security policies") distributed by Cisco's ISGs or iWAGs. At install time, you need to determine what policy enforcement points your installation use and what features you need to install. PEPS might be: • Cisco ISG pool • Cisco ASR 5K • Cisco ASR9K • MAG • IWAG • Cisco WLC • SCE Device Pool • RADIUS AAA server or device pool • Procera • Allot • PDSN • PCEF Consult your Cisco technical representative for configuring a custom site. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 200 (last accessed June 18, 2021).

<table>
<tr>
<td></td>
<td>


See SP WiFi: Deploying Access for 3G and 4G Mobile Networks, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 65 (last accessed June 18, 2021) (describing ISG authorization flow).
</td>
</tr>
<tr>
<td>**10[F]** enforcing said appropriate security policies at said at least one PEF in respect of access by the multimodal device to the converged network.</td>
<td>Cisco's SP Wi-Fi enforces said appropriate security policies at said at least one PEF in respect of access by the multimodal device to the converged network.

Further, Cisco's SP Wi-Fi (via, e.g., the WAG) applies a subscriber enforcement policy based on the subscriber's profile (e.g., "enforcing said appropriate security policies at said at least one PEF in respect of access by the multimodal device to the converged network").</td>
</tr>
</table>

	 *See TECSPM* at 34. Cisco ISG/WAG (i.e., the policy manager and the policy enforcement point (PEF)) provide policy management services for different access networks as well as policy enforcement functions. 

See SP WiFi: Deploying Access for 3G and 4G Mobile Networks, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 27 (last accessed June 18, 2021) (describing ISG and IOS relationship with regards to policy management).

The ISG/WAG acts as a policy manager as well as the policy enforcement point (PEF). The Policy management function within the ISG/WAG decides the policies for user access. For example, the policy manager (i.e., ISG/WAG) decides whether to create a dedicated (complete) or a minimal (lite) session.

Dedicated Sessions

A dedicated or regular session is a full-fledged Intelligent Services Gateway (ISG) subscriber session. All subscriber sessions that are authenticated cause the creation of dedicated sessions on ISG. The policy manager of ISG decides whether to create a complete session context (a dedicated session) or a minimal session context (a lite session).

Note ISG provides high availability support for converted (lite to dedicated) unclassified and DHCPv4 sessions.

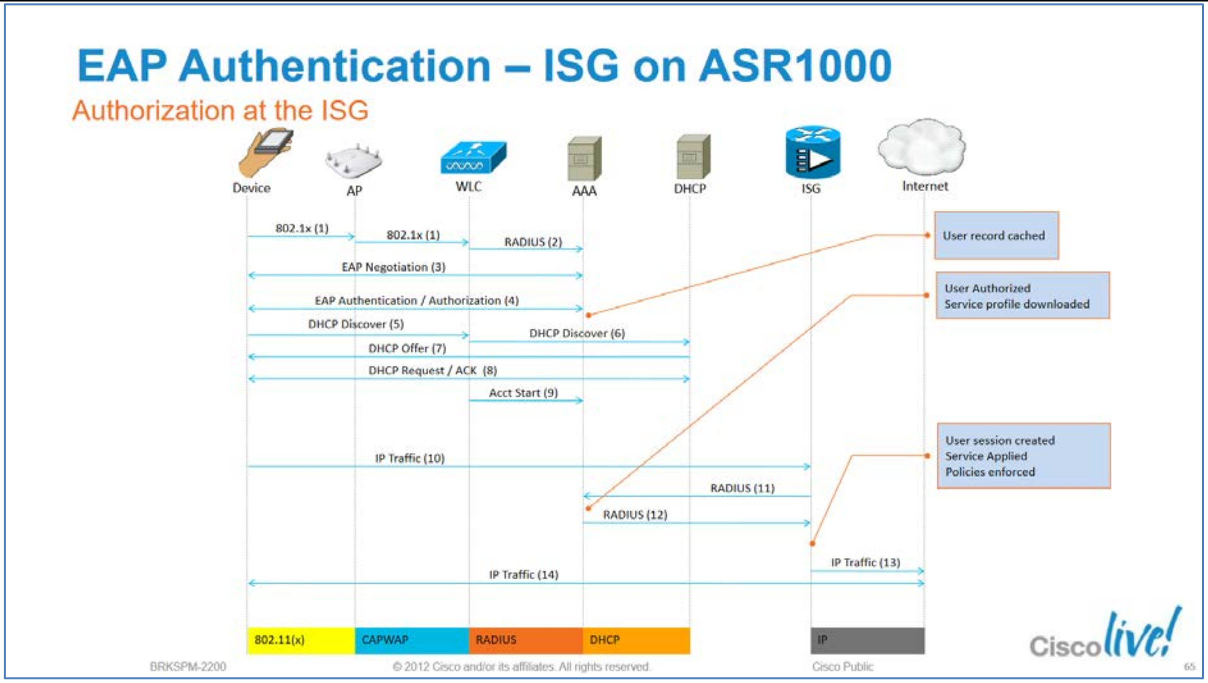
Supported Triggers

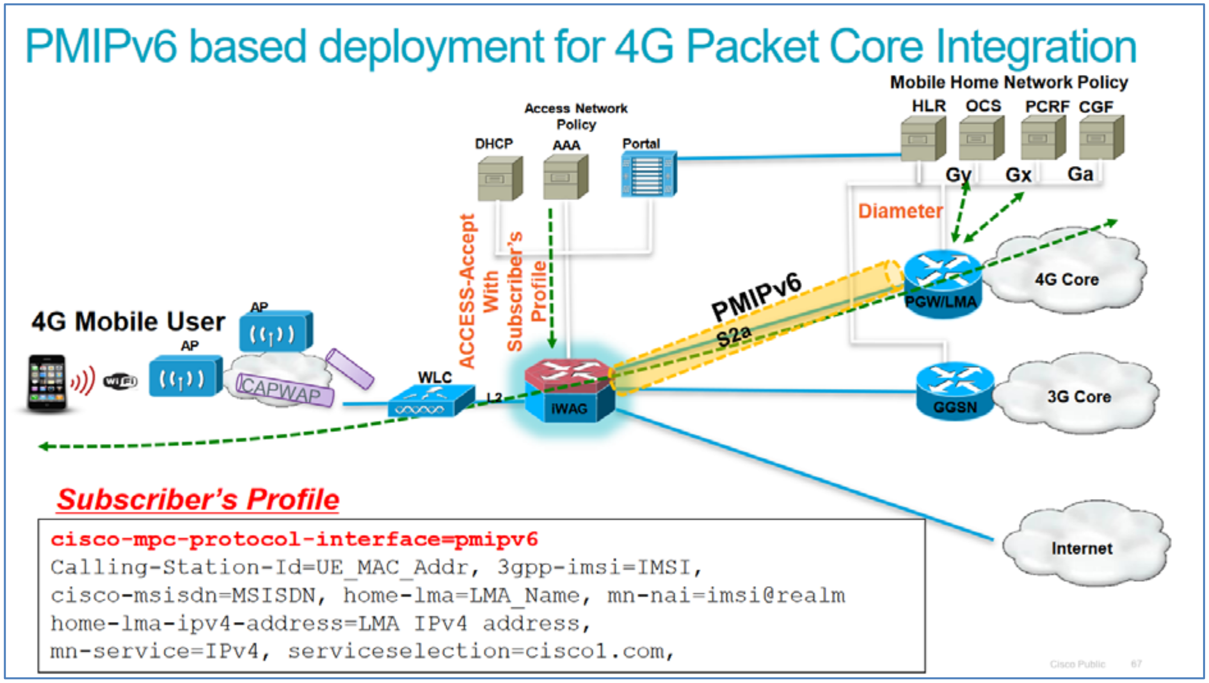
Walk-by sessions can be created through any of the following session initiators:

- Packet trigger: Here the session creation is triggered by a subscriber's IP packet having an unclassified IP address or MAC address.
- RADIUS proxy: This trigger is commonly used in PWLAN deployments where ISG acts as a RADIUS proxy. Here, the session creation is triggered by the subscriber's RADIUS packets.
- DHCP: This trigger is another SIP used in a few PWLAN deployments. Here, the session creation is triggered by the subscriber's DHCP control packets.
- EoGRE walkby: When ISG is configured for EoGRE, DHCP control packets and unclassified MAC packets on the EoGRE interface trigger session creation on ISG.

See Intelligent Services Gateway Configuration Guide Cisco IOS XE Release 3S, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-3s/isg-xe-3s-book/isg-wlkby-supp.html, at 27 (last accessed June 18, 2021).

	Within the ISG/WAG, the policy manager distributes the policies to the policy enforcement point (PEF) to enforce them for a user. A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however. Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 199 (last accessed June 18, 2021).

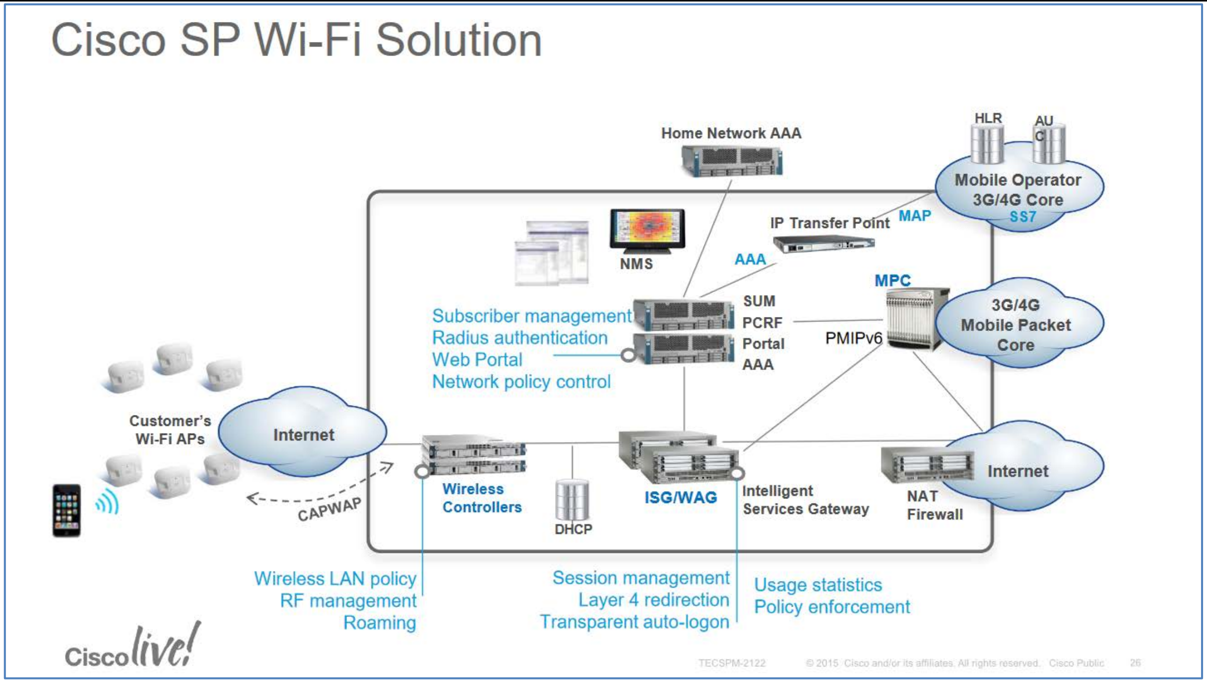
	 *See SP WiFi: Deploying Access for 3G and 4G Mobile Networks*, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 65 (last accessed June 18, 2021) (describing ISG authorization flow for multimodal devices).
CLAIM 11	
11[A] A method according to claim 10 wherein said inter-technology change-off message comprises a user ID	Cisco's SP Wi-Fi provides a method according to claim 10 wherein said inter-technology change-off message comprises a user ID identifying a subscriber, and at least one of a device ID, a second access technology indicator, and a first access technology indicator. Cisco's SP Wi-Fi subscriber profiles include a cisco-msisdn attribute (e.g., "a user ID identifying a subscriber") and a Calling-Station-Id attribute (e.g., "at least one of a device ID"). Additionally, on information and belief,

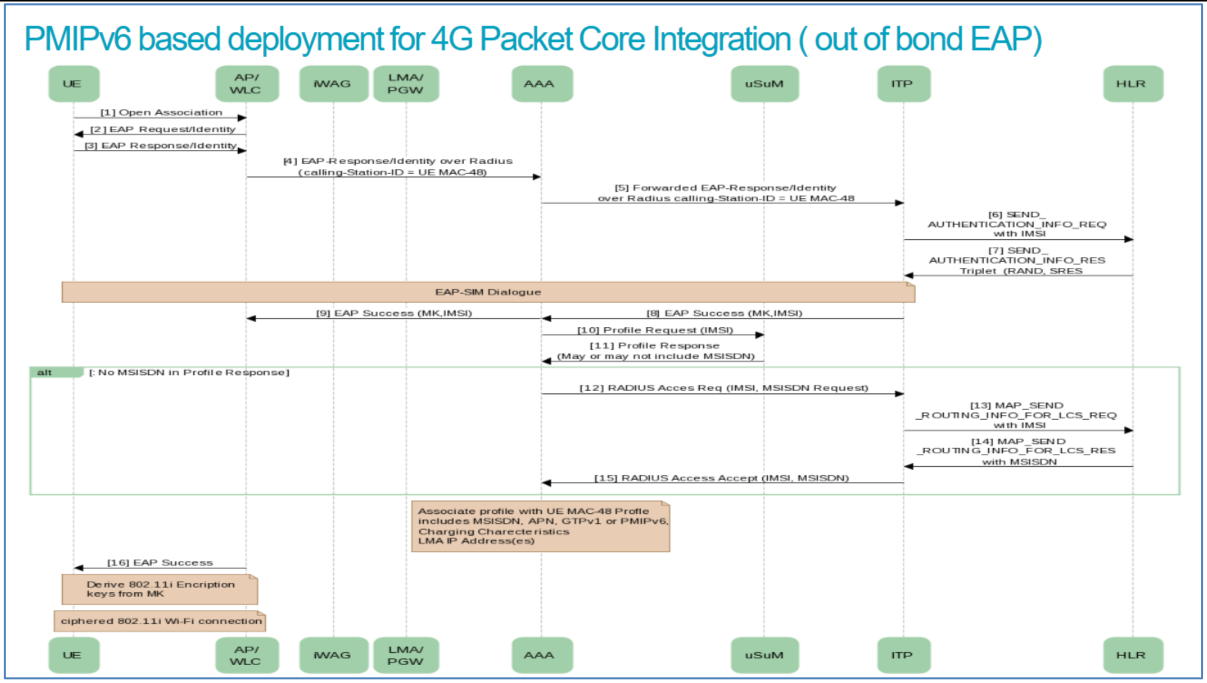
identifying a subscriber, and at least one of a device ID, a second access technology indicator, and a first access technology indicator.	Cisco's SP Wi-Fi subscriber profiles includes a Cisco-Service-Selection attribute ("a second access technology indicator") and ("a first access technology indicator"). *See Cisco Wireless Controller Configuration Guide, Release 8.2*, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_0101010.html (last accessed June 18, 2021).  *See TECSPM* at 67 (generally describing subscriber profile structure for 4G Packet Core).
CLAIM 12	
12[A] A method according to claim 11 further comprising:	Cisco's SP Wi-Fi provides a method according to claim 11 that further comprises the elements set forth below.

12[B] looking up, in a subscriber database, by the policy manager, subscriber security parameters of a subscriber identified in the inter-technology change-off message; and	Cisco's SP Wi-Fi provides a method according to claim 11 further comprising looking up, in a subscriber database, by the policy manager, subscriber security parameters of a subscriber identified in the inter-technology change-off message. Cisco's SP Wi-Fi iWAG(s) look up, in subscriber profile repository (SPR), subscriber security parameters of a subscriber identified in a DHCP message (e.g., " looking up, in a subscriber database, by the policy manager, subscriber security parameters of a subscriber identified in the inter-technology change-off message"). **Revised: February 24, 2013, OL-29745-03** Cisco Policy Suite adapts to a variety of sources for subscriber data. Possible subscriber profile repositories (SPR) that may be available to you are: • Cisco Control Center interface component of CPS • Cisco's Unified Subscriber Manager (Cisco Unified SuM) component of CPS • Cisco's AAA server component of CPS • LDAP • AAA This flexibility lets you include either an external subscriber management system in your Cisco Policy Builder architecture or the internal, integrated Cisco Unified SuM. Subscriber management schemes vary and are particular to an individual network. Because of this, the procedures for obtaining subscriber data are discussed in the specific documents that matches your network architecture. See your specific document. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 209 (last accessed June 18, 2021).

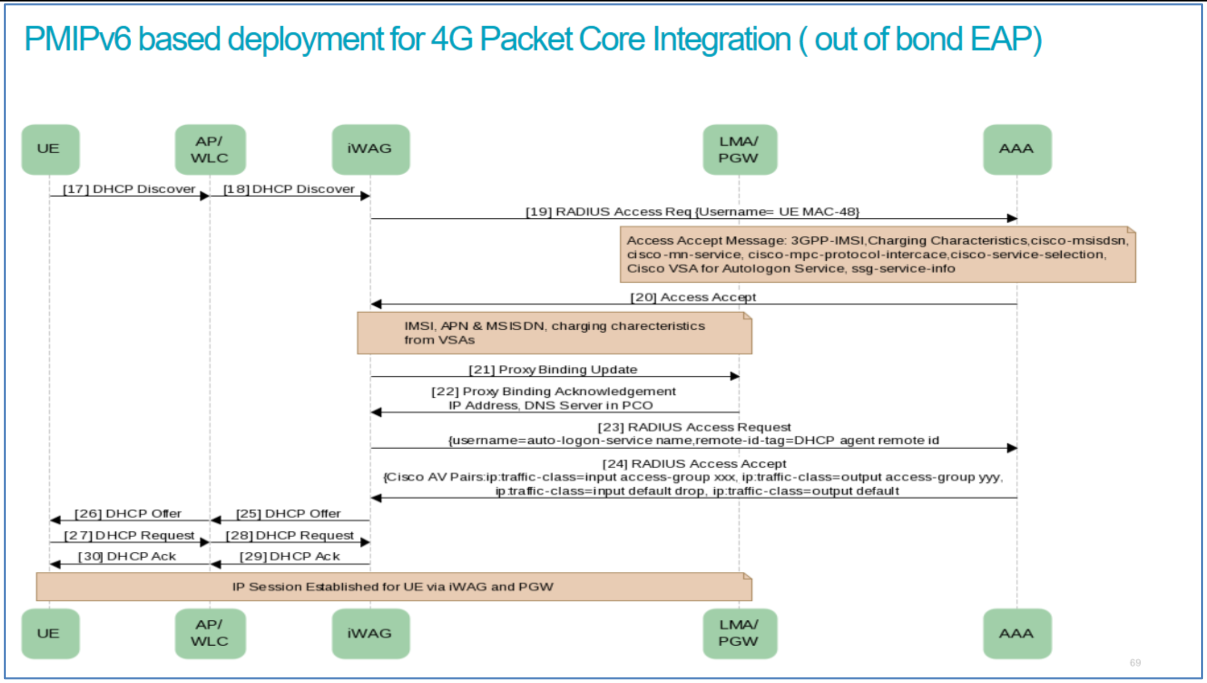
12[C] searching said policy database, by said policy manager, for a user policy corresponding to said subscriber.	Cisco's SP Wi-Fi provides a method according to claim 11 further comprising searching said policy database, by said policy manager, for a user policy corresponding to said subscriber. For example, Cisco's SP Wi-Fi iWAG(s) search a policy database for a user policy corresponding to said subscriber (e.g., "searching said policy database, by said policy manager, for a user policy corresponding to said subscriber"). A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however. Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource. *See id*. at 199.
CLAIM 14	
14[A] A method according to claim 10 wherein the step of detecting occurrence of an inter-technology change-off occurs at one of a layer 2 monitoring level and a higher than layer 2 monitoring level.	Cisco's SP Wi-Fi provides a method according to claim 10 wherein the step of detecting occurrence of an inter-technology change-off occurs at one of a layer 2 monitoring level and a higher than layer 2 monitoring level. For example, Cisco's SP Wi-Fi APs and/or WLCs (e.g., "ICME") perform the method of claim 10 including detecting occurrence of an inter-technology change-off occurring at one of a layer 2 monitoring entity and a higher than layer 2 monitoring entity.

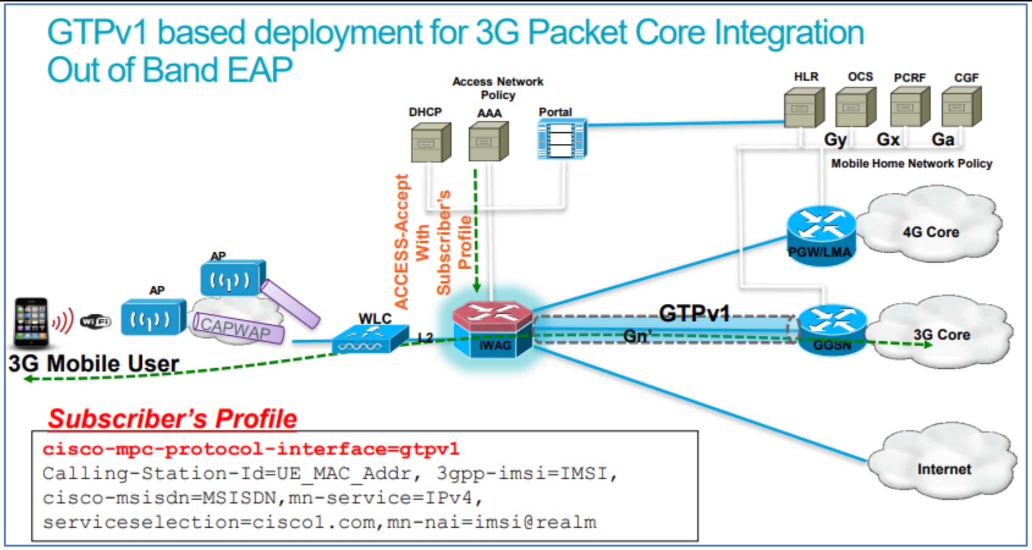
	Cisco Unified Wireless Network Security Solutions The Cisco Unified Wireless Network supports Layer 2 and Layer 3 security methods. • Layer 2 security • Layer 3 security (for WLAN) or Layer 3 security (for Guest LAN) *See, e.g.*, *Wireless LAN Controller Layer 2 Layer 3 Security Compatibility Matrix*, CISCO, https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106082-wlc-compatibility-matrix.html (last accessed June 18, 2021) (describing, based on a Cisco 4400/2100 Series WLC, various Layer 2 and Layer 3 security methods supported on the Wireless LAN Controller).
CLAIM 15	
15[A] A method according to claim 14 wherein detecting occurrence of an inter-technology change-off occurs at a layer 2 monitoring level, wherein the inter-technology change-off is between UMTS and WLAN, and wherein the inter-technology change-off is detected when an association occurs.	Cisco's SP Wi-Fi provide a method according to claim 14 wherein detecting occurrence of an inter-technology change-off occurs at a layer 2 monitoring level, wherein the inter-technology change-off is between UMTS and WLAN, and wherein the inter-technology change-off is detected when an association occurs. For example, Cisco's SP Wi-Fi APs or WLCs (e.g., "the ICME") are connected to by user equipment (UE). The ICME detects the inter-technology change-off of the UE from a first access technology (e.g., 3G/4G) of the converged network to a second access technology (e.g., Wi-Fi) of the converged network and transmits a DHCP message (e.g., "detecting occurrence of an inter-technology change-off occurs at a layer 2 monitoring level, wherein the inter-technology change-off is between UMTS and WLAN, and wherein the inter-technology change-off is detected when an association occurs"). *See TECSPM* at 26, 68-69 (disclosing Cisco's UE to WLAN handover process in the Cisco SP Wi-Fi system).

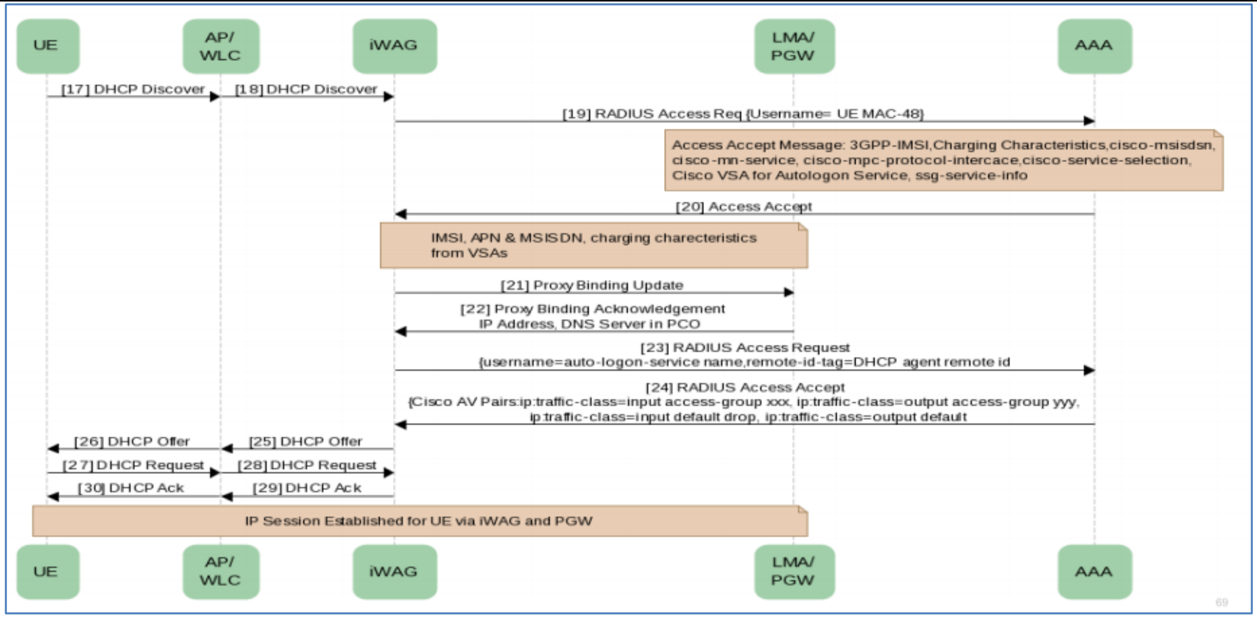
	Cisco SP Wi-Fi Solution Home Network AAA HLR AUC Mobile Operator 3G/4G Core SS7 MAP IP Transfer Point NMS AAA MPC SUM PCRF Portal AAA PMIPv6 3G/4G Mobile Packet Core Subscriber management Radius authentication Web Portal Network policy control Customer's Wi-Fi APs Internet CAPWAP Wireless Controllers DHCP ISG/WAG Intelligent Services Gateway NAT Firewall Internet Wireless LAN policy RF management Roaming Session management Layer 4 redirection Transparent auto-logon Usage statistics Policy enforcement Cisco live! *Id*. at 26.


PMIPv6 based deployment for 4G Packet Core Integration (out of bond EAP)
UE
AP/ WLC
iWAG
LMA/ PGW
AAA
uSuM
ITP
HLR
[1] Open Association
[2] EAP Request/Identity
[3] EAP Response/Identity
[4] EAP-Response/Identity over Radius (calling-Station-ID = UE MAC-48)
[5] Forwarded EAP-Response/Identity over Radius calling-Station-ID = UE MAC-48
[6] SEND_ AUTHENTICATION_INFO_REQ with IMSI
[7] SEND_ AUTHENTICATION_INFO_RES Triplet (RAND, SRES
EAP-SIM Dialogue
[9] EAP Success (MK,IMSI)
[8] EAP Success (MK,IMSI)
[10] Profile Request (IMSI)
[11] Profile Response (May or may not include MSISDN)
alt
[: No MSISDN in Profile Response]
[12] RADIUS Acces Req (IMSI, MSISDN Request)
[13] MAP_SEND _ROUTING_INFO_FOR_LCS_REQ with IMSI
[14] MAP_SEND _ROUTING_INFO_FOR_LCS_RES with MSISDN
[15] RADIUS Access Accept (IMSI, MSISDN)
Associate profile with UE MAC-48 Profile includes MSISDN, APN, GTPv1 or PMIPv6, Charging Charecteristics LMA IP Address(es)
[16] EAP Success
Derive 802.11i Encription keys from MK
ciphered 802.11i Wi-Fi connection
UE
AP/ WLC
iWAG
LMA/ PGW
AAA
uSuM
ITP
HLR

Id. at 68.

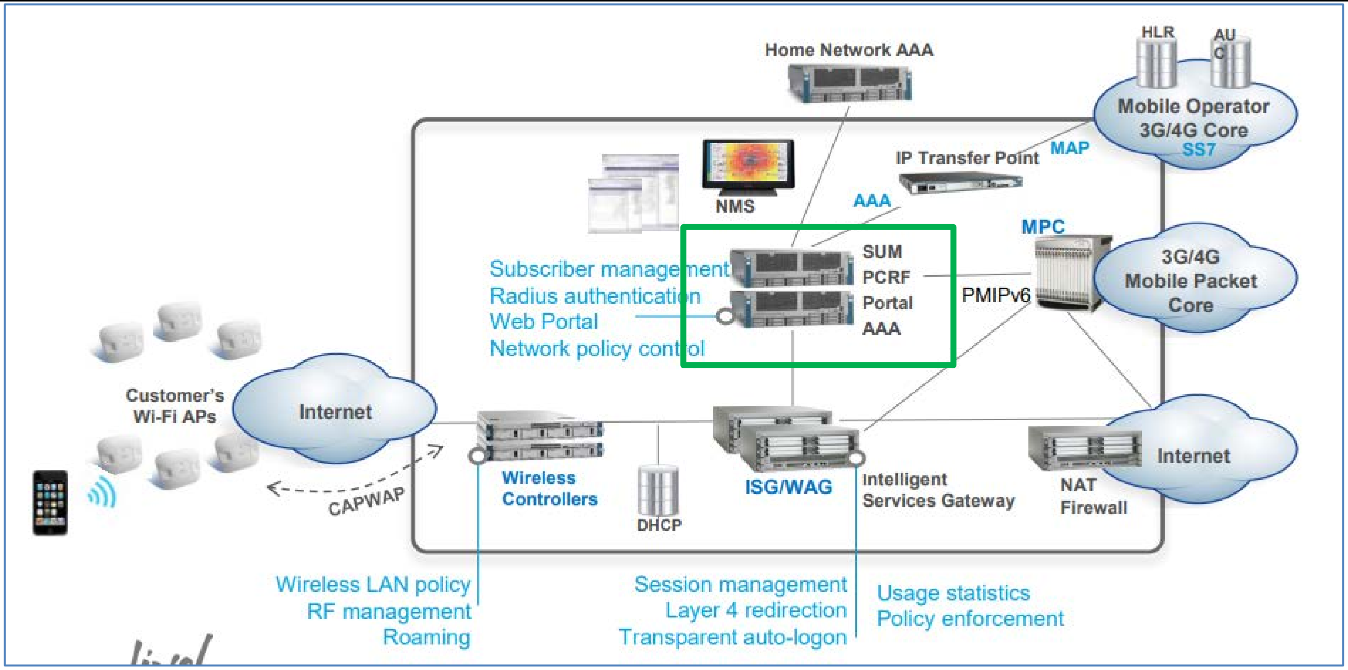
	 *Id.* at 69.
CLAIM 16	
16[A] A method according to claim 14 wherein detecting occurrence of an inter-technology change-off occurs at a layer 3 monitoring level, wherein the inter-	Cisco's SP Wi-Fi provides a method according to claim 14 wherein detecting occurrence of an inter-technology change-off occurs at a layer 3 monitoring level, wherein the inter-technology change-off is between UMTS and WLAN, and wherein the change-off is detected on an occurrence of a change in an IP address allocated to the multimodal device, receipt of a message from the multimodal mobile device, receipt of a DHCP message, or any other mechanism from the network or device to initiate a layer 3 handoff or change-off. Cisco's SP Wi-Fi supports ICME (i.e., handover) between, as one non-limiting example, 3G (i.e., UMTS) and Wi-Fi (i.e., WLAN) access networks.

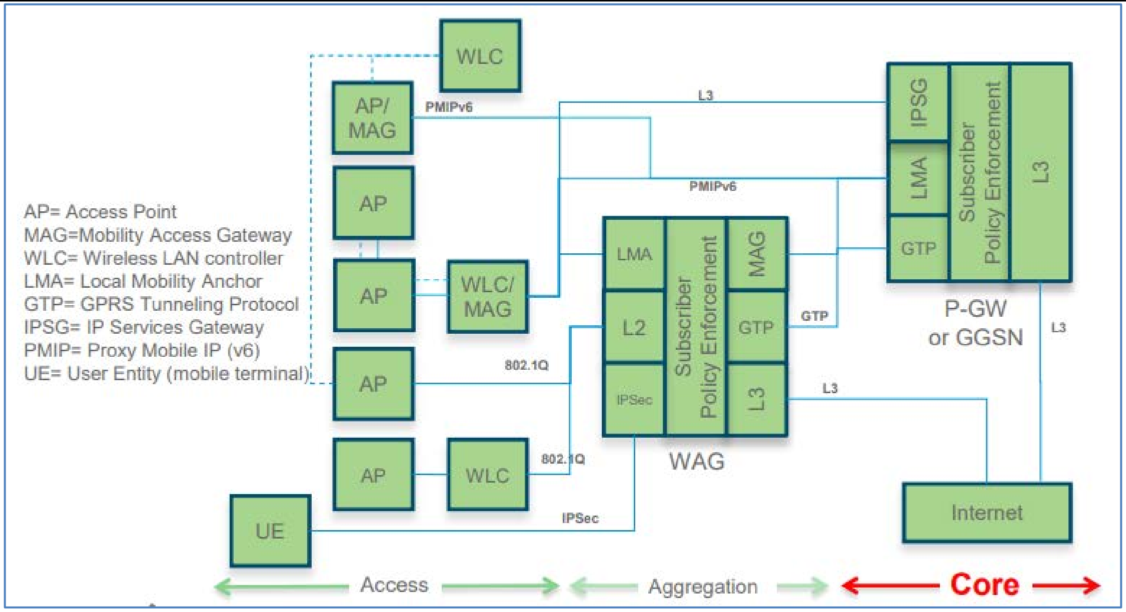
technology change-off is between UMTS and WLAN, and wherein the change-off is detected on an occurrence of a change in an IP address allocated to the multimodal device, receipt of a message from the multimodal mobile device, receipt of a DHCP message, or any other mechanism from the network or device to initiate a layer 3 handoff or change-off.	 *See TECSPM* at 62. The WLC (e.g., "the ICME is a layer 3 monitoring entity") detects the inter-technology handover of the UE via a DHCP message when the UE is associated with the Wi-Fi access network (e.g., "inter-technology change-off is between UMTS and WLAN and wherein the change-off is detected on an occurrence of a change in an IP address allocated to the multimodal device, receipt of a message from the multimodal mobile device, receipt of a DHCP message, or any other mechanism from the network or device to initiate a layer 3 handoff or change-off"). *Id.* at 69.



Id. at 69.

CLAIM 17	
17[A] A method according to claim 10 wherein said appropriate policy is a combination of said user policy and said access technology policy, and wherein portions of said appropriate policies are distributed to	Cisco's SP Wi-Fi provides a method according to claim 10 wherein said appropriate policy is a combination of said user policy and said access technology policy, and wherein portions of said appropriate policies are distributed to each PEF of said at least one PEF. User-enforced policies (i.e., appropriate policy) are the combination of applicable network policies (i.e., said access technology policy) and subscriber enforcement policies (i.e., user policy).

each PEF of said at least one PEF.	 *See TECSPM* at 26. Further, Cisco's SP Wi-Fi (via, e.g., the WAG) applies a subscriber enforcement policy based on the subscriber's profile.

	 *Id*. at 34. Cisco ISG/WAG (i.e., the policy manager and the policy enforcement point (PEF)) provide policy management services for different access networks as well as policy enforcement functions. 

See SP WiFi: Deploying Access for 3G and 4G Mobile Networks, CISCO, https://www.cisco.com/c/dam/global/en_ca/assets/plus/assets/pdf/CiscoPlus-SP-WiFi-Deployment-SWOOD.pdf, at 27 (last accessed June 18, 2021).

The ISG/WAG act as a policy manager as well as the policy enforcement point (PEF). The Policy management function within the ISG/WAG decides the policies for user access. For example, the policy manager (i.e., ISG/WAG) decides whether to create a dedicated (complete) or a minimal (lite) session.

Dedicated Sessions

A dedicated or regular session is a full-fledged Intelligent Services Gateway (ISG) subscriber session. All subscriber sessions that are authenticated cause the creation of dedicated sessions on ISG. The policy manager of ISG decides whether to create a complete session context (a dedicated session) or a minimal session context (a lite session).

Note ISG provides high availability support for converted (lite to dedicated) unclassified and DHCPv4 sessions.

Supported Triggers

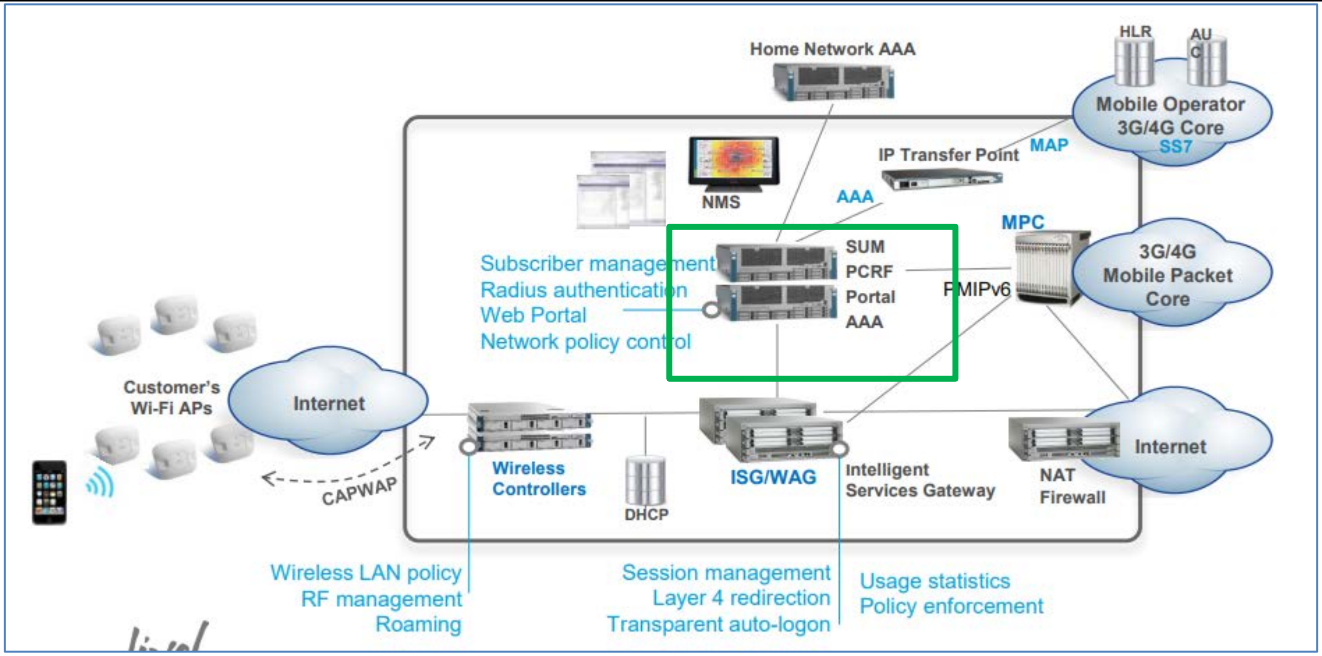
Walk-by sessions can be created through any of the following session initiators:

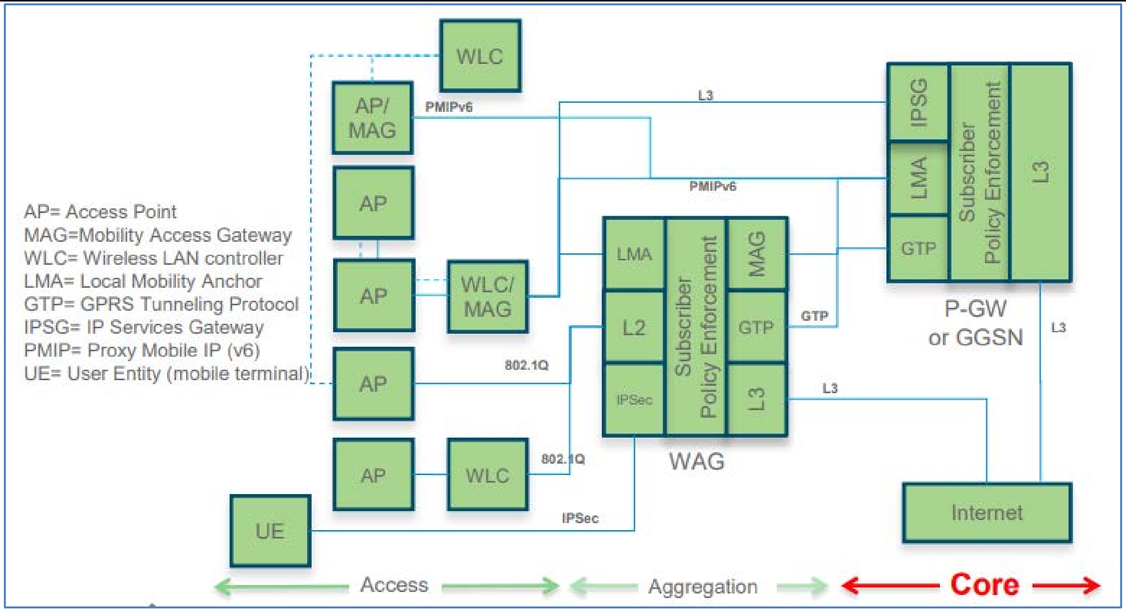
- Packet trigger: Here the session creation is triggered by a subscriber's IP packet having an unclassified IP address or MAC address.
- RADIUS proxy: This trigger is commonly used in PWLAN deployments where ISG acts as a RADIUS proxy. Here, the session creation is triggered by the subscriber's RADIUS packets.
- DHCP: This trigger is another SIP used in a few PWLAN deployments. Here, the session creation is triggered by the subscriber's DHCP control packets.
- EoGRE walkby: When ISG is configured for EoGRE, DHCP control packets and unclassified MAC packets on the EoGRE interface trigger session creation on ISG.

See Intelligent Services Gateway Configuration Guide Cisco IOS XE Release 3S, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-3s/isg-xe-3s-book/isg-wlkby-supp.html (last accessed June 18, 2021).

Within the ISG/WAG, the policy manager distributes the policies to the policy enforcement point (PEF) to enforce them for a user, as explained below.

	A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however. Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes.Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf , at 200 (last accessed June 18, 2021).
CLAIM 18	
18[A] A method according to claim 17 wherein said combination of said user policy and said access technology policy is a sum of said user policy plus said access technology policy.	Cisco's SP Wi-Fi provides a method according to claim 17 wherein said combination of said user policy and said access technology policy is a sum of said user policy plus said access technology policy. Cisco's SP Wi-Fi WAG applies a user policy which is the combination of an applicable network policy and a subscriber enforcement policy (e.g., "wherein said combination of said user policy and said access technology policy is a sum of said user policy plus said access technology policy"). *See TECSPM* at 26, 34.

	Home Network AAA HLR Mobile Operator 3G/4G Core SS7 MAP IP Transfer Point NMS AAA MPC SUM PCRF Portal AAA PMIPv6 3G/4G Mobile Packet Core Subscriber management Radius authentication Web Portal Network policy control Customer's Wi-Fi APs Internet CAPWAP Wireless Controllers DHCP ISG/WAG Intelligent Services Gateway NAT Firewall Internet Wireless LAN policy RF management Roaming Session management Layer 4 redirection Transparent auto-logon Usage statistics Policy enforcement *Id*. at 26.

	WLC AP/ MAG PMIPv6 L3 IPSG LMA GTP Subscriber Policy Enforcement L3 PMIPv6 AP AP= Access Point MAG=Mobility Access Gateway WLC= Wireless LAN controller LMA= Local Mobility Anchor GTP= GPRS Tunneling Protocol IPSG= IP Services Gateway PMIP= Proxy Mobile IP (v6) UE= User Entity (mobile terminal) AP WLC/ MAG LMA L2 IPSec Subscriber Policy Enforcement MAG GTP L3 GTP P-GW or GGSN L3 802.1Q AP L3 AP WLC 802.1Q WAG Internet UE IPSec Access Aggregation Core *Id*. at 34.

	Cisco Policy Suite adapts to a variety of sources for subscriber data. Possible subscriber profile repositories (SPR) that may be available to you are: • Cisco Control Center interface component of CPS • Cisco's Unified Subscriber Manager (Cisco Unified SuM) component of CPS • Cisco's AAA server component of CPS • LDAP • AAA This flexibility lets you include either an external subscriber management system in your Cisco Policy Builder architecture or the internal, integrated Cisco Unified SuM. Subscriber management schemes vary and are particular to an individual network. *See Cisco Policy Suite 5.5.3 Wi-Fi Configuration Guide*, CISCO, https://www.cisco.com/c/dam/en/us/td/docs/wireless/quantum-policy-suite/R5-5-3/CPS5-5-3Wi-FiConfigurationGuide.pdf, at 209 (last accessed June 18, 2021).

	The Initial Blueprint executes the following policy flow. • Pre-Session Policies. These are policies not associated with a subscriber session. They are defined in the "Pre-session policies". • Load Session. Upon receiving a policy message, the load session policies attempt to load the session using keys that are retrieved from the input message. • Stop Session. Upon loading a session, the session can be stopped if "Stop session" criteria is fulfilled (for example, a RADIUS stop message can be a stop session criteria). • Start Session. If a session does not exist, then a new session can be started if the "Start session" criteria is fulfilled (for example, a RADIUS start message can be a start session criteria). • Active Session Policies. If a session is active then the active session policies are initiated. The active session policies are executed in the following order: – Map session data from input. This maps data from the input record to the network session (for example, mapping the user ID from a RADIUS record). *Id.* at 213. The Network Session node is always part of the Initial Blueprint. This node describes the data you want to capture for each subscriber's session. The Initial Blueprint defines the set of attributes used in the NetworkSession that are common across all network sessions. These attributes can be: • macAddress—the MAC address of the device connected to the network • userId—the user ID of the subscriber connected to the network • framedIp—the framed IP of the subscriber's network connection • circuitId—the circuit ID of the subscriber's network connection • avps—the list of AVPs (attribute value pairs) associated with the subscriber's network session • devices—the list of network devices associated with the subscriber's network session *Id.* at 228.

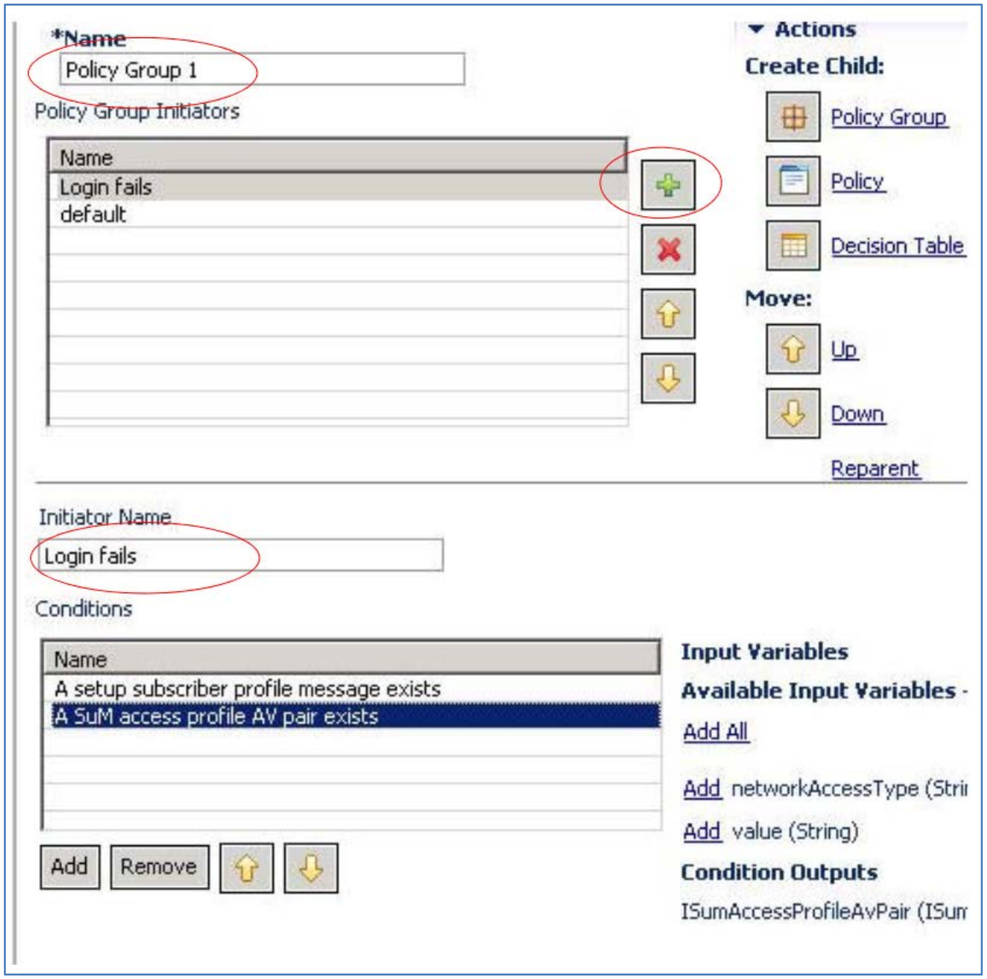
	 *Id*. at 251 (portraying configuration of user policies combining network access policies and subscriber policies).

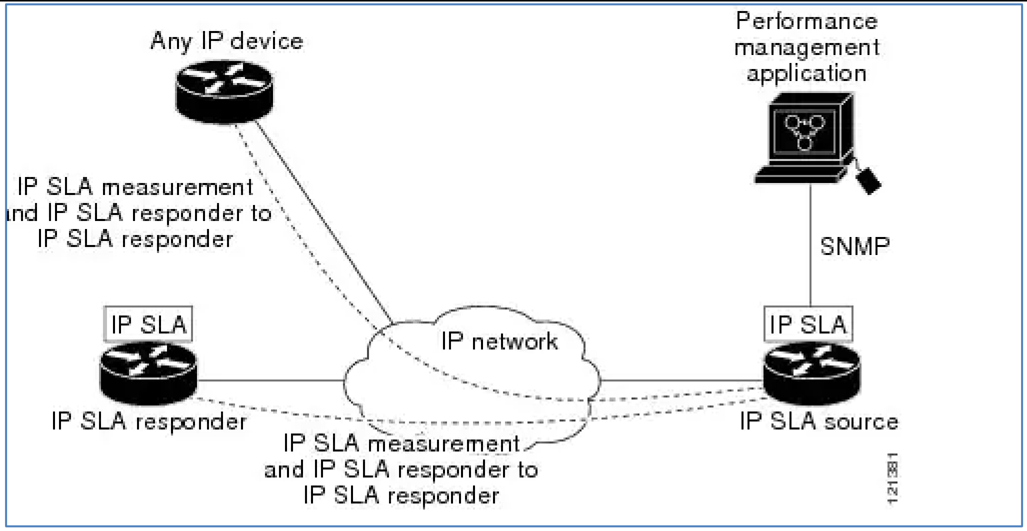
EXHIBIT D

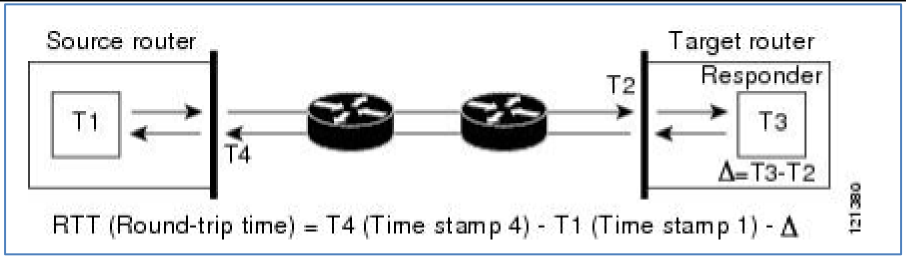
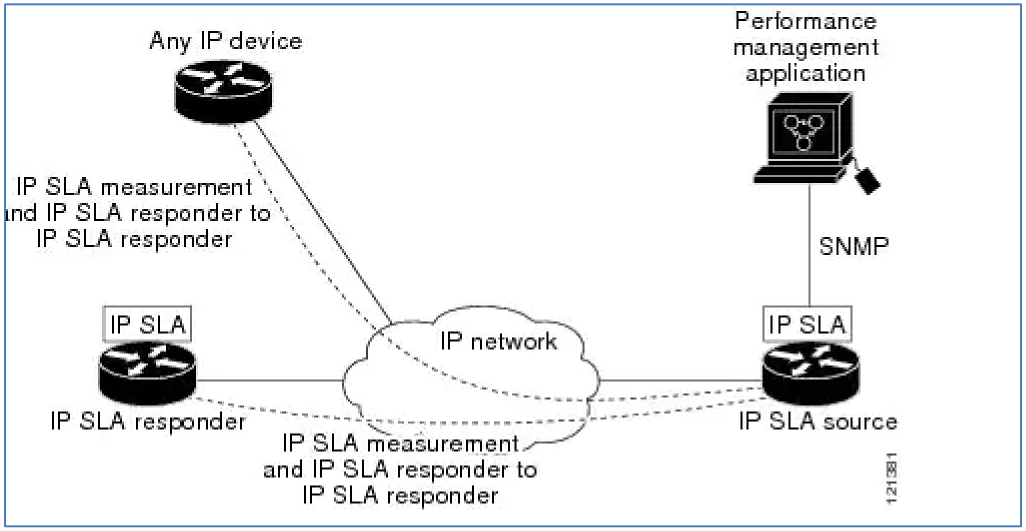
EXHIBIT D

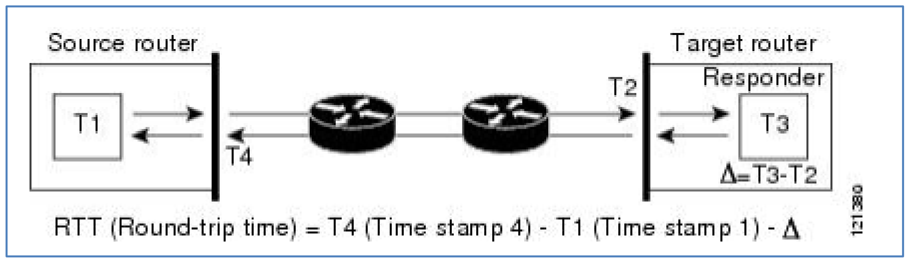
U.S. Patent No. 8,665,733 v. Cisco Routers and Switches

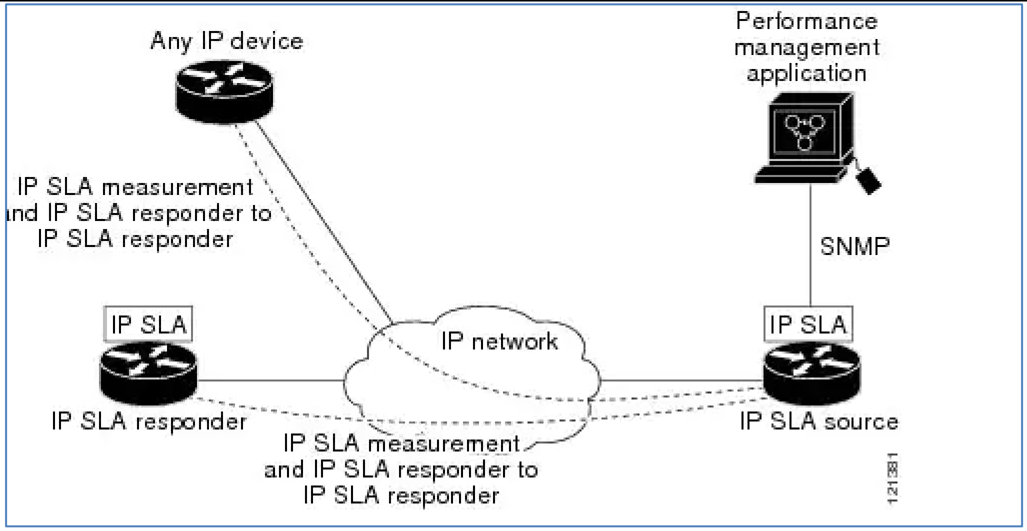
U.S. Patent No. 8,665,733	Application to Cisco Routers and Switches
CLAIM 1	
1[Pre.] A method for apportioning delays of a plurality of network elements on a round trip path in a network, said method comprising the steps of:	To any extent the preamble is limiting, Cisco routers and switches that implement IP Service Level Agreements ("IP SLAs"), including, but not limited to, Cisco 800 Series Industrial Integrated Services Routers, Cisco 800M Integrated Services Router, Cisco 1000 Series Connected Grid Routers, Cisco 2000 Series Connected Grid Routers, Cisco Catalyst 9200 Series Switches, Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, Cisco Catalyst 9500 Series Switches, and Cisco Catalyst 9600 Series Switches (hereafter "Cisco Routers and Switches"), practice a method for apportioning delays of a plurality of network elements on a round trip path in a network comprising the steps set forth below. For example, "Cisco IP SLAs uses active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. IP SLAs sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services and collects network performance information in real time. The information collected includes data about response time, one-way latency, jitter (interpacket delay variance), packet loss, voice quality scoring, network resource availability, application performance, and server response time. IP SLAs performs active monitoring by generating and analyzing traffic to measure performance either between Cisco devices or from a Cisco device to a remote IP device such as a network application server. Measurement statistics provided by the various IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies." *IP SLAs Configuration Guide, Cisco IOS Release 15M&T*, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_overview-0.pdf, at 1 (Nov. 21, 2012) (last accessed June 20, 2021).

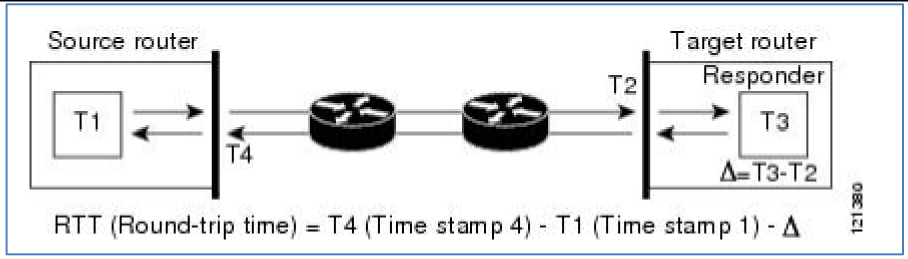
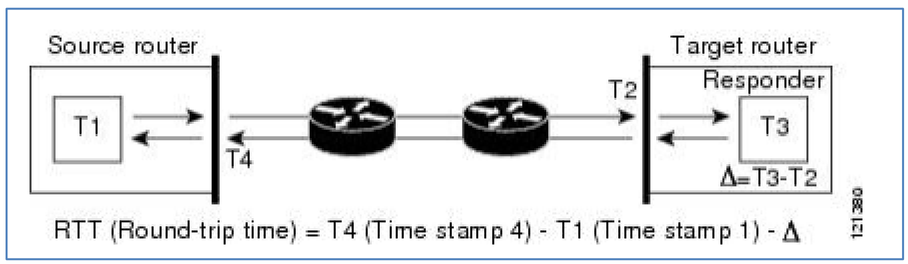
	What is IP SLA IP SLA is an active method of monitoring and reliably reporting on network performance. By "active," I refer to the fact that IP SLA will generate and actively monitor traffic continuously across the network. An IP SLA Router is capable of generating traffic and reporting on it in real time. IP SLA can be configured in such a way that it can report on statistics such as: • Jitter • Response time • Packet loss • Voice Quality Scoring (MOS) • Connectivity • Server or website responses and downtime • Delay *IP SLA Fundamentals*, CISCO, https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (last accessed June 20, 2021).
1[A] Transmitting, at a user element, a loopback packet having a probe session indicator along said round trip path,	Cisco Routers and Switches include a method comprising the step of transmitting, at a user element (e.g., IP SLA router), a loopback packet (e.g., IP SLA test packets) having a probe session indicator (e.g., using time stamping) along said round trip path, as shown below. For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *IP SLA Fundamentals*, CISCO, https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (last accessed June 20, 2021).

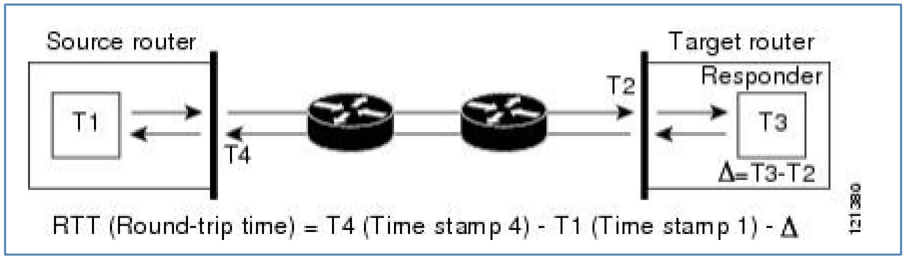
	 *IP SLAs Configuration Guide, Cisco IOS Release 15M&T*, CISCO, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_overview-0.pdf, at 5 (Nov. 21, 2012) (last accessed June 20, 2021). The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take timestamps from sending, processing, to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

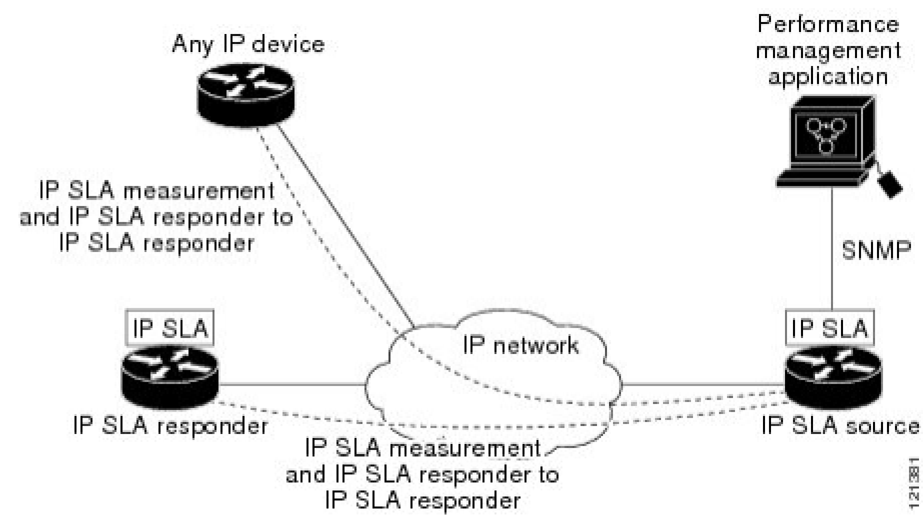
	 *Id.* at 7.
1[B] wherein said roundtrip path reaches a core network element, and	Cisco Routers and Switches transmit a loopback packet (e.g., IP SLA test packets) having a probe session indicator (e.g., using time stamping) along a round trip path, wherein said roundtrip path reaches a core network element (e.g., IP SLA Responder). For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *Id.*  *Id.* at 5.

	The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
1[C] wherein the loopback packet is received at said user element after completing said roundtrip path;	Cisco Routers and Switches transmit a loopback packet (e.g., IP SLA test packets) that is received at the user element (e.g., IP SLA router) after completing said roundtrip path as shown below. For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *Id.*

	 *Id.* at 5. The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

	 *Id.* at 7.
1[D] determining at each of said plurality of network elements on said round trip path the presence of said probe session indicator, and	Cisco Routers and Switches determine at each of said plurality of network elements on said round trip path the presence of said probe session indicator by using time stamping, as shown below. For example, "[t]he figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
1[E] responsive to the presence of said probe session	Cisco Routers and Switches include the step where responsive to the presence of said probe session indicator, logging a first timestamp corresponding to the time of receipt of said loopback message, and a second timestamp corresponding to the time of retransmission of said loopback message, as shown below.

indicator, logging a first timestamp corresponding to the time of receipt of said loopback message, and a second timestamp corresponding to the time of retransmission of said loopback message; and	For example, "[w]hen enabled, the IP SLAs Responder allows the target device to take two time stamps both when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time." *Id.* at 6. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
1[F] transmitting at each of said plurality of network elements said first and second timestamps to a network management system.	Cisco Routers and Switches transmit at each of said plurality of network elements said first and second timestamps to a network management system, as shown below. For example, "SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IP SLAs operations running on the Cisco devices." *Id.* at 2. "After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP." *Id.* at 4–5.

<table>
<tr><td></td><td>

To implement IP SLAs network performance measurement you need to perform these tasks:
1 Enable the IP SLAs Responder, if appropriate.
2 Configure the required IP SLAs operation type.
3 Configure any options available for the specified IP SLAs operation type.
4 Configure threshold conditions, if required.
5 Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6 Display and interpret the results of the operation using Cisco software commands or an NMS system with SNMP.
Id. at 5.</td></tr>
<tr><td colspan="2">**CLAIM 2**</td></tr>
<tr><td>**2** A method for apportioning delays as claimed in</td><td>Cisco Routers and Switches practice a method for apportioning delays as claimed in claim 1, *see supra* 1[Pre.]-1[F], wherein they determine at each of a plurality of network elements on round trip path the presence of said probe session indicator by using time stamping in an application layer of the network element, for example:</td></tr>
</table>

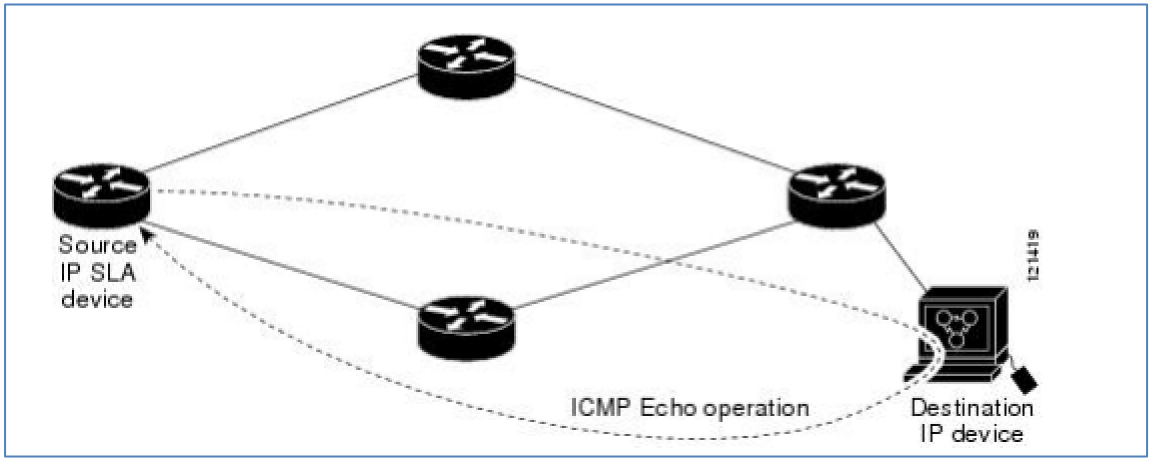
claim 1 wherein said determining the presence of said probe session indicator is determined in an application layer of said network element.	"Depending on the specific IP SLAs operation, statistics of delay, packet loss, jitter, packet sequence, connectivity, path, server response time, and download time can be monitored within the Cisco device and stored in both CLI and SNMP MIBs. The packets have configurable IP and application layer options such as a source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), a Virtual Private Network (VPN) routing/forwarding instance (VRF), and a URL web address." *Id.* at 2.
CLAIM 4	
4 A method for apportioning delays as claimed in claim 2 wherein said probe session indicator comprises a probe bit identifying a probe session.	Cisco Routers and Switches practice a method for apportioning delays as claimed in claim 2, *see supra* 2, wherein, on information and belief, said probe session indicator comprises a probe bit identifying a probe session. For example: "The IP SLAs Probe Enhancements feature is an application-aware synthetic operation agent that monitors network performance by measuring response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, for problem analysis, and for designing network topologies." *Id.* at 4.
CLAIM 5	
5 A method for apportioning delays as claimed in	Cisco Routers and Switches include a method for apportioning delays as stated in claim 4, *see supra* 4, wherein said probe bit comprises a bit in a message header of said loopback message, as shown below.

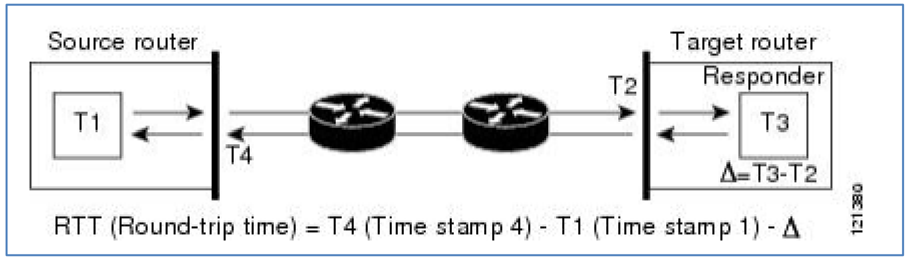
claim 4 wherein said probe bit comprises a bit in a message header of said loopback message.	For example, "[e]ach ICMP packet includes a sequence number in its header that is used to count the number of packets received out of sequence on the sender. Both the sequence number and the receive timestamps can be used to calculate out-of-sequence packets on the source-to-destination path. If the receive time stamp for a packet is greater than that of the next packet, the first packet was delivered out of order on the source-to-destination path. For the destination-to-source path, the same method can be applied. Note that if the packet is out of order on the source-to-destination path, it should be returned out of order to the sender unless there is also misordering on the destination-to-source path." *Id.* at 203.

Step 12	Do one of the following:
	• **tos** *number*
	• **traffic-class** *number*
	
	Example:
	`Device(config-ip-sla-jitter)# tos 160`
	
	Example:
	`Device(config-ip-sla-jitter)# traffic-class 160`
		(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
		or
		(Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.

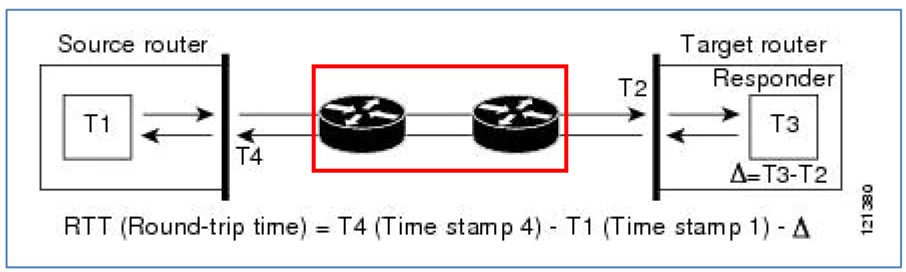
Step 13	**flow-label** *number* **Example:** `Device(config-ip-sla-jitter)# flow-label 112233`	(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.

Id. at 128.

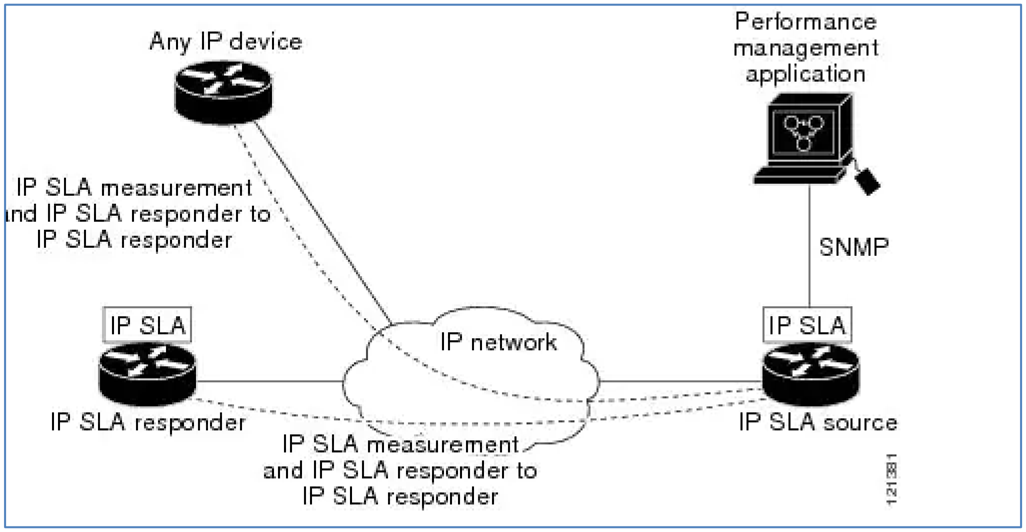
CLAIM 6	
6 A method for apportioning delays as claimed in claim 1 wherein said loopback message comprises a modified Internet Control Message Protocol (ICMP) PING message, and wherein said loopback message has identical uplink and downlink paths.	Cisco Routers and Switches include a method for apportioning delays as claimed in claim 1, *see supra* 1[Pre.]-1[F], wherein said loopback message comprises a modified Internet Control Message Protocol (ICMP) PING message, and wherein said loopback message has identical uplink and downlink paths, as shown below. "In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements." *Id.* at 290.  *Id.* The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source

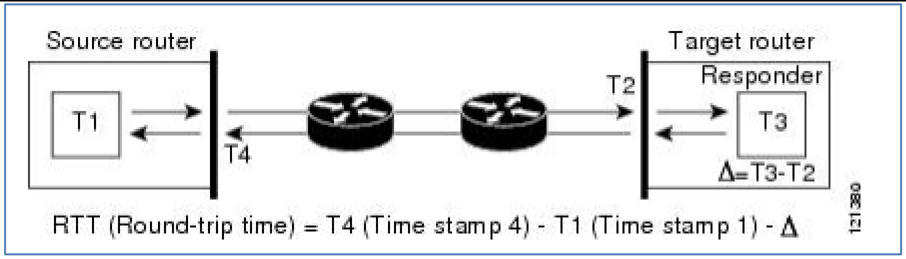
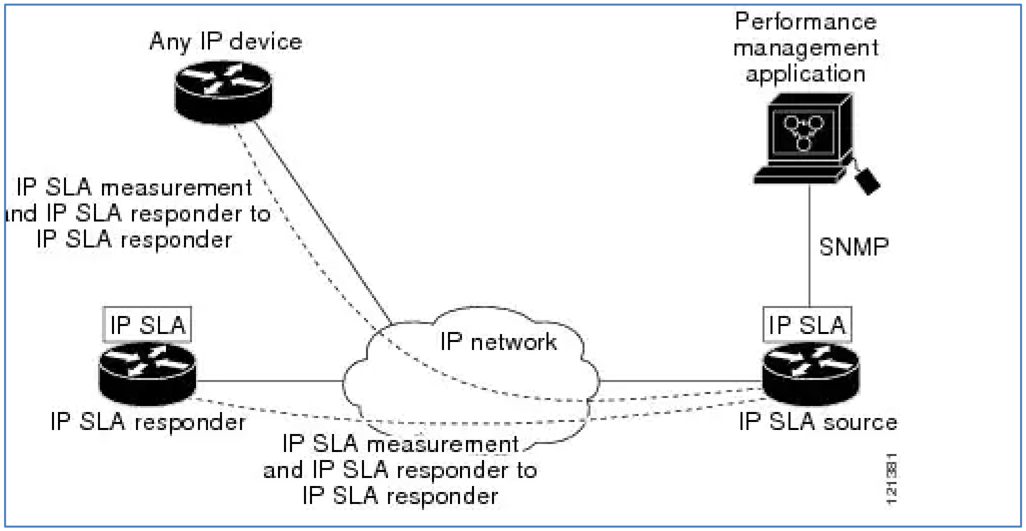
<table>
<tr><td></td><td>device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.” Id. at 6–7.


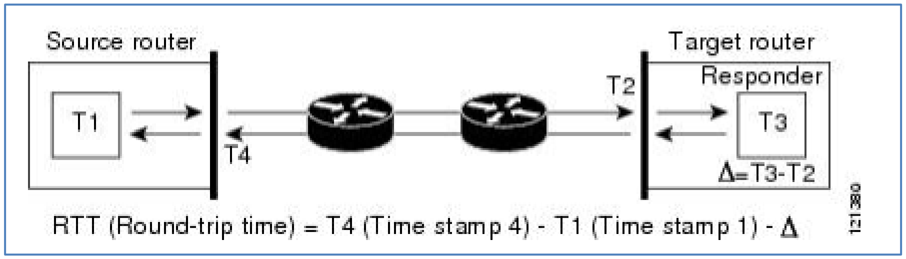
Id. at 7.</td></tr>
<tr><td colspan="2">CLAIM 7</td></tr>
<tr><td>7[Pre.] A method performed by an intermediate network device, the method comprising:</td><td>To any extent the preamble is limiting, the Cisco Routers and Switches include a method performed by an intermediate network device, as shown below.

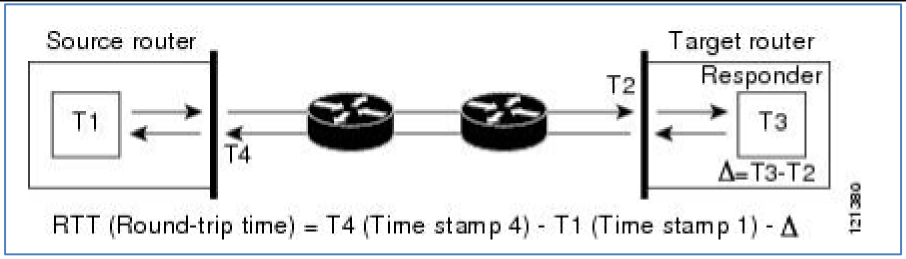
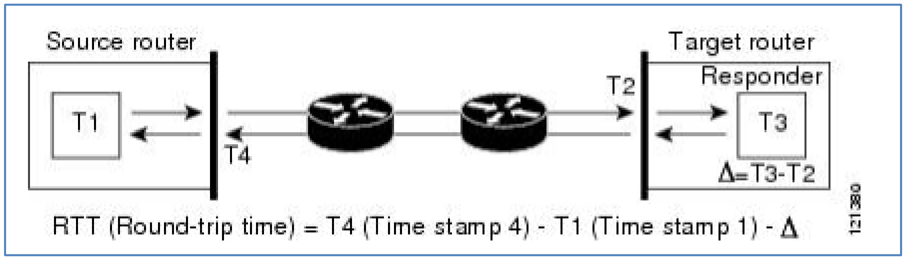
For example, Cisco IP SLAs send data across the network to measure the performance between multiple network locations or across multiple network paths. The multiple network locations or paths include several intermediate devices as shown below.


Id. (emphasis added).</td></tr>
<tr><td>7[A] receiving, at the intermediate</td><td>Cisco Routers and Switches include a method comprising the step of receiving, at the intermediate network device, a message having a probe session indicator, as shown below.</td></tr>
</table>

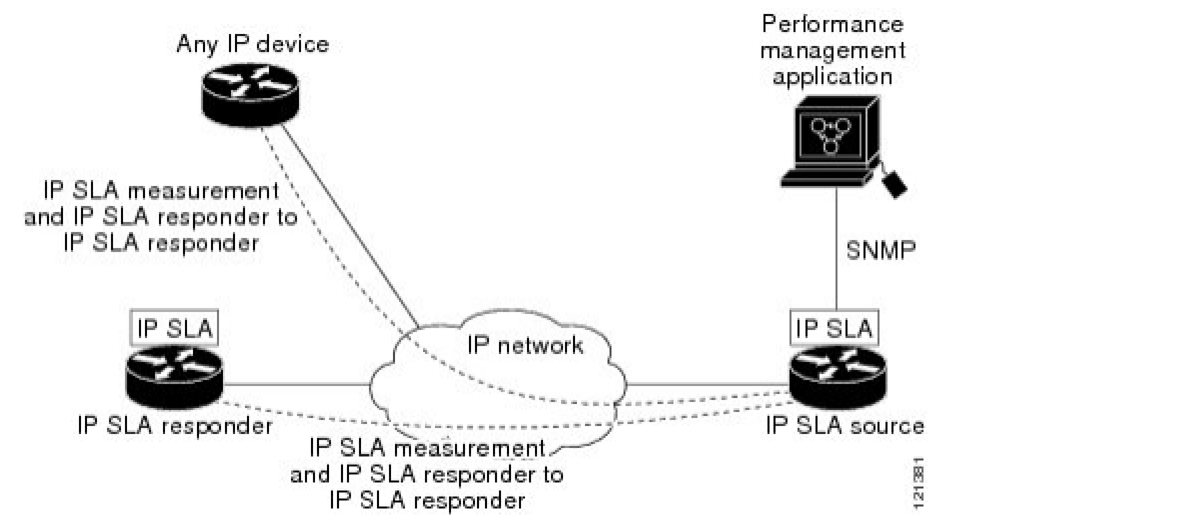
network device, a message having a probe session indicator,	For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *Id.*  *Id.* at 5. The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) through the intermediate network device and back again from the target router to the source router through the intermediate network device. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

	 *Id.* at 7.
7[B] wherein the message is a loopback message having an uplink path originating from a user element that reaches a network core element and a downlink path returning the loopback message to the user element;	Cisco Routers and Switches include a method comprising the step of receiving, at the intermediate network device, a message having a probe session indicator, wherein the message is a loopback message having an uplink path originating from a user element that reaches a network core element and a downlink path returning the loopback message to the user element. For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *Id.*  *Id.* at 5.

	The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) through the intermediate network device and back again from the target router to the source router through the intermediate network device. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
7[C] determining that the message includes the probe session indicator;	Cisco Routers and Switches determine that the message includes the probe session indicator by using time stamping, as shown below. For example, "[t]he figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

	 *Id.* at 7.
7[D] based on the message including the probe session indicator: generating a first timestamp corresponding to a time of receipt of the message: generating a second timestamp corresponding to a time of transmission of the message, and	Cisco Routers and Switches include the step where based on the message including the probe session indicator: generating a first timestamp corresponding to a time of receipt of the message and generating a second timestamp corresponding to a time of transmission of the message. For example, "[w]hen enabled, the IP SLAs Responder allows the target device to take two time stamps both when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time." *Id.* at 6. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.

7[E] transmitting the first timestamp and the second timestamp to a first device; and	Cisco Routers and Switches transmit the first timestamp and the second timestamp to a first device (e.g., Network Management System). For example, "SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IPSLAs operations running on the Cisco devices. For a complete description of the object variables referenced by the IP SLAs feature, refer to the text of the CISCO-RTTMON-MIB.my file, available from the Cisco MIB website." *Id*. at 2. "After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP." *Id.* at 4–5.

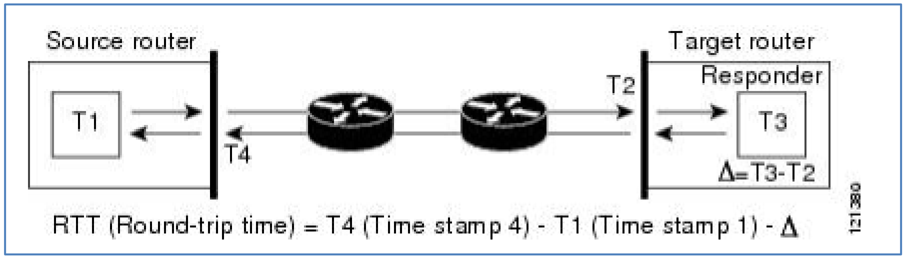
<table>
<tr>
<td></td>
<td>


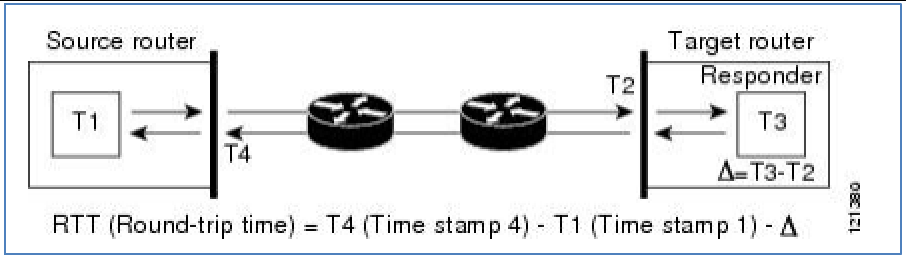
To implement IP SLAs network performance measurement you need to perform these tasks:

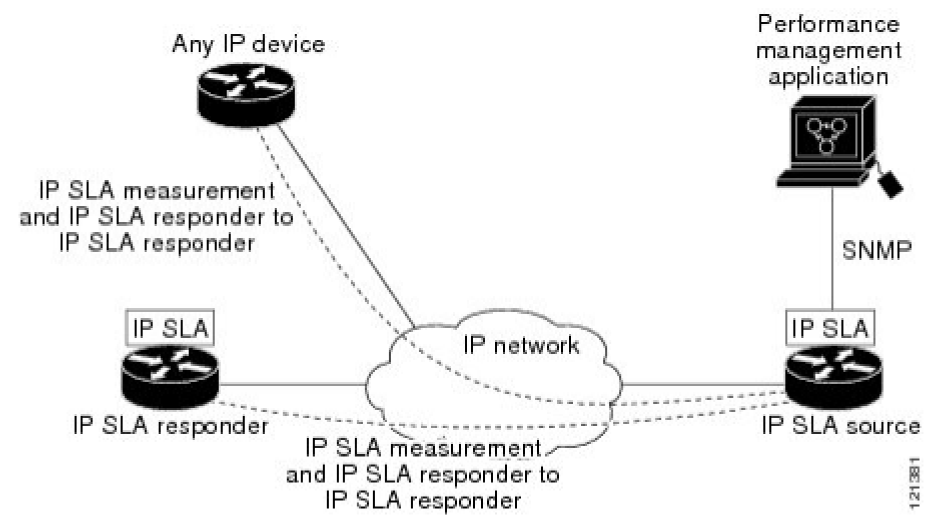
1 Enable the IP SLAs Responder, if appropriate.
2 Configure the required IP SLAs operation type.
3 Configure any options available for the specified IP SLAs operation type.
4 Configure threshold conditions, if required.
5 Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6 Display and interpret the results of the operation using Cisco software commands or an NMS system with SNMP.

Id. at 5.
</td>
</tr>
<tr>
<td>7[F] transmitting the message to a second device.</td>
<td>Cisco Routers and Switches transmit the message to a second device (e.g., network elements).

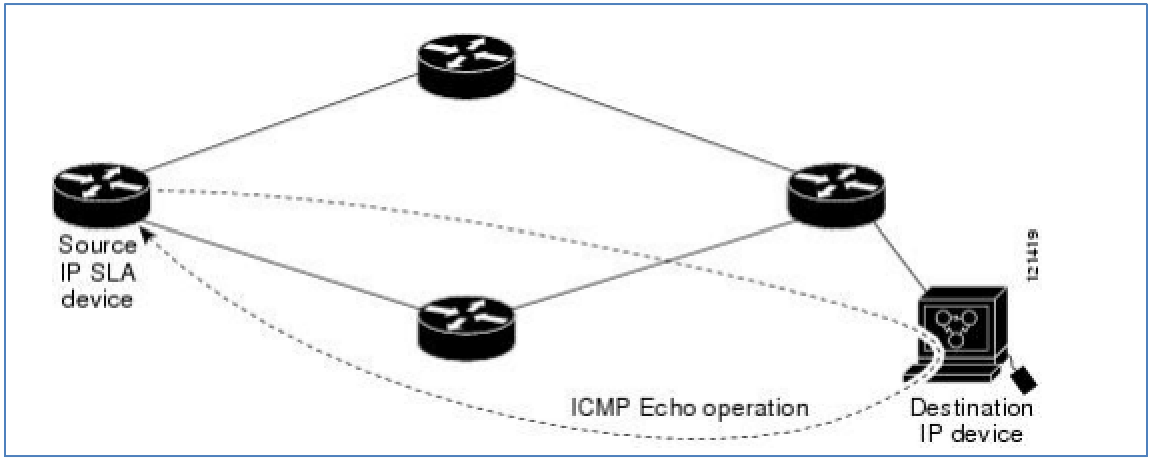
For example, the IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example:</td>
</tr>
</table>

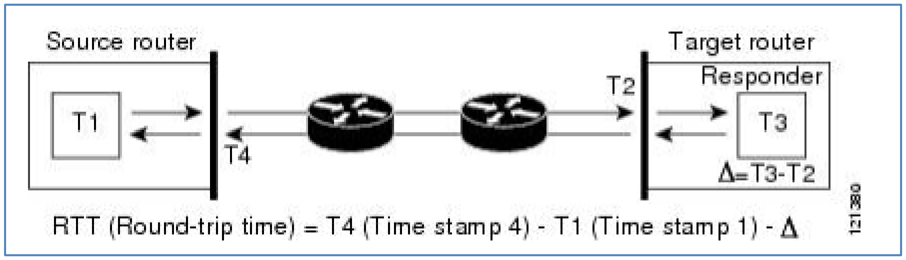
	"The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
CLAIM 8	
8 The method of claim 7, wherein said loopback message traverses the same intermediate nodes on the uplink path and downlink path.	Cisco Routers and Switches include the method of claim 7, *see supra* 7, wherein said loopback message traverses the same intermediate nodes on the uplink path and downlink path. For example, the IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

	 *Id.* at 7.
CLAIM 9	
9 The method of claim 7, wherein the first device is a network management system.	Cisco Routers and Switches include the method of claim 7, *see supra* 7, wherein the first device is a network management system. For example, "SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IPSLAs operations running on the Cisco devices. For a complete description of the object variables referenced by the IP SLAs feature, refer to the text of the CISCO-RTTMON-MIB.my file, available from the Cisco MIB website." *Id.* at 2. "After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP." *Id.* at 4–5.

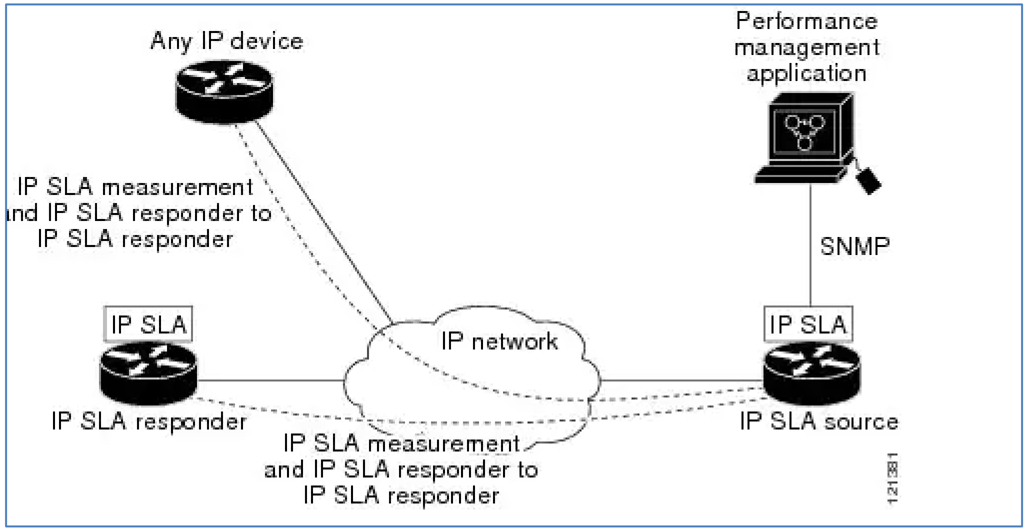
	 To implement IP SLAs network performance measurement you need to perform these tasks: **1** Enable the IP SLAs Responder, if appropriate. **2** Configure the required IP SLAs operation type. **3** Configure any options available for the specified IP SLAs operation type. **4** Configure threshold conditions, if required. **5** Schedule the operation to run, then let the operation run for a period of time to gather statistics. **6** Display and interpret the results of the operation using Cisco software commands or an NMS system with SNMP. *Id.* at 5.

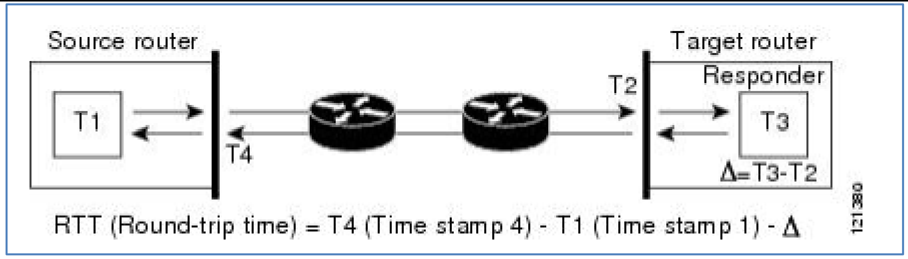
CLAIM 10	
10 The method of claim 7, wherein determining that the message includes the probe session indicator is performed at an application layer of the intermediate network device.	Cisco Routers and Switches include the method of claim 7, *see supra* 7, wherein determining that the message includes the probe session indicator is performed at an application layer of the intermediate network device. For example: "Depending on the specific IP SLAs operation, statistics of delay, packet loss, jitter, packet sequence, connectivity, path, server response time, and download time can be monitored within the Cisco device and stored in both CLI and SNMP MIBs. The packets have configurable IP and application layer options such as a source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), a Virtual Private Network (VPN) routing/forwarding instance (VRF), and a URL web address." *Id*. at 2.
CLAIM 12	
12 The method of claim 7, wherein the probe session indicator comprises a probe bit identifying a probe session.	Cisco Routers and Switches include the method of claim 7, *see supra* 7, wherein, on information and belief, the probe session indicator comprises a probe bit identifying a probe session. For example: "The IP SLAs Probe Enhancements feature is an application-aware synthetic operation agent that monitors network performance by measuring response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, for problem analysis, and for designing network topologies." *Id*. at 4.

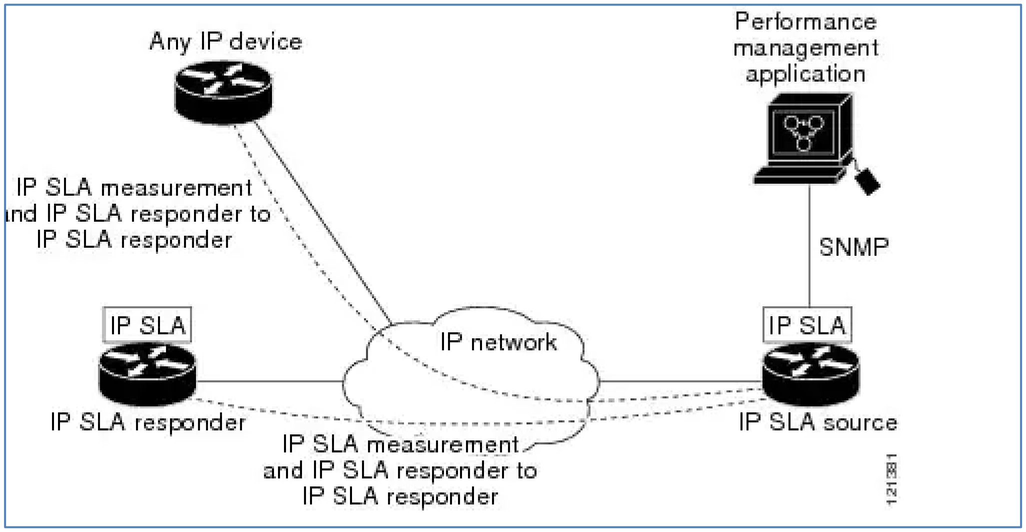
CLAIM 13	
13 The method of claim 7, wherein the message comprises a modified Internet Control Message Protocol (ICMP) PING message.	Cisco Routers and Switches include the method of claim 7, *see supra* 7, wherein the message comprises a modified Internet Control Message Protocol (ICMP) PING message. For example: "In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements." *Id.* at 290.  *Id.* The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source

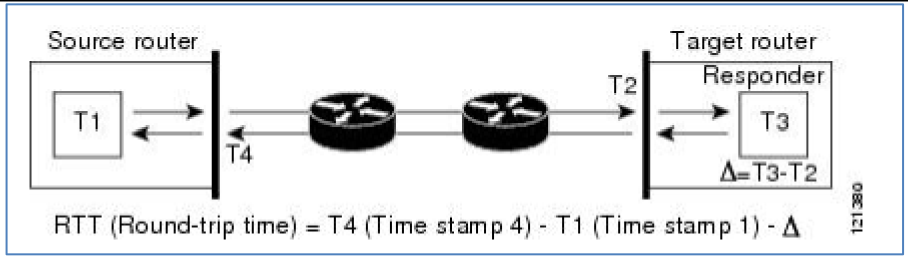
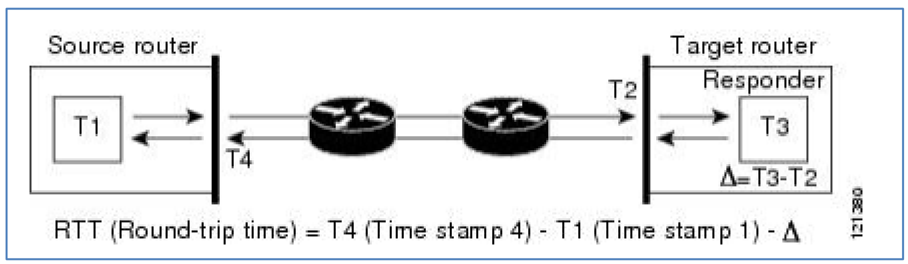
	device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
CLAIM 14	
14[Pre.] An intermediate network device comprising:	To any extent the preamble is limiting, Cisco Routers and Switches include an intermediate network device comprising the following elements, as shown below.
14[A] a memory device; and	Cisco Routers and Switches include an intermediate network device that comprises a memory device. For example: "The IP SLAs multiple operations scheduling functionality allows you to schedule multiple IPSLAs operations as a group, using the following configuration parameters: …. Ageout--Amount of time to keep the operation in memory when it is not actively collecting information. By default, the operation remains in memory indefinitely." *Id.* at 376. "Because the responder cannot directly read the video packets, the responder creates two queues and a block of reallocated memory for use by both video sink and the responder itself." *Id.* at 75. "When a packet arrives at video sink, it is processed to extract the sequence numbers and time stamps, and that information is put into one of the pre-allocated memory blocks. A pointer to this block is put into the used queue for later processing by the main responder task." *Id.*

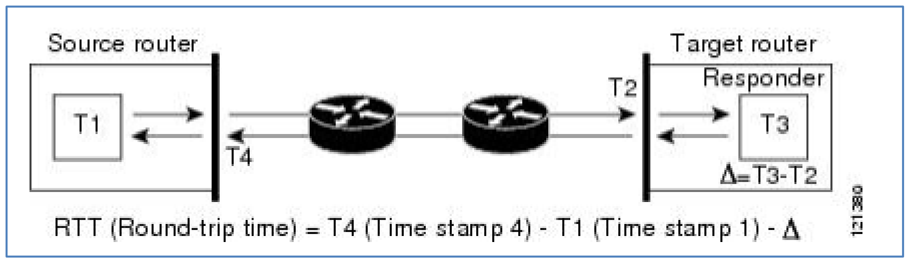
	"At periodic timer intervals, the responder processes a number of the packet information blocks from the used queue and updates the statistics appropriately. When the data is processed, the blocks are returned to the free-memory list to be used again." *Id.*
14[B] a processor in communication with the memory device, the processor being configured to:	Cisco Routers and Switches include an intermediate network device comprising a processor in communication with the memory device, wherein the processor is configured to perform the functions identified below. "Devices may take tens of milliseconds to process incoming packets, due to other high-priority processes. This delay affects the response times because the reply to test packets might be sitting on queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if IP SLAs Responder is being used), in order to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays." *Id.* at 6. "When a packet arrives at video sink, it is processed to extract the sequence numbers and time stamps, and that information is put into one of the pre-allocated memory blocks. A pointer to this block is put into the used queue for later processing by the main responder task." *Id.* at 75. "At periodic timer intervals, the responder processes a number of the packet information blocks from the used queue and updates the statistics appropriately. When the data is processed, the blocks are returned to the free-memory list to be used again." *Id.* "Having the Receive and Transmit timestamps allows the IP SLA packet to not only measure the RTT of the packet getting from the source to the destination, but also to record how long the destination device takes to process the packet." *IP SLA Fundamentals*, CISCO, https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (last accessed June 20, 2021).
14[C] receive a message having a probe session indicator,	Cisco Routers and Switches include an intermediate network device comprising a processor in communication with the memory device, the processor being configured to receive a message having a probe session indicator. For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *Id.*

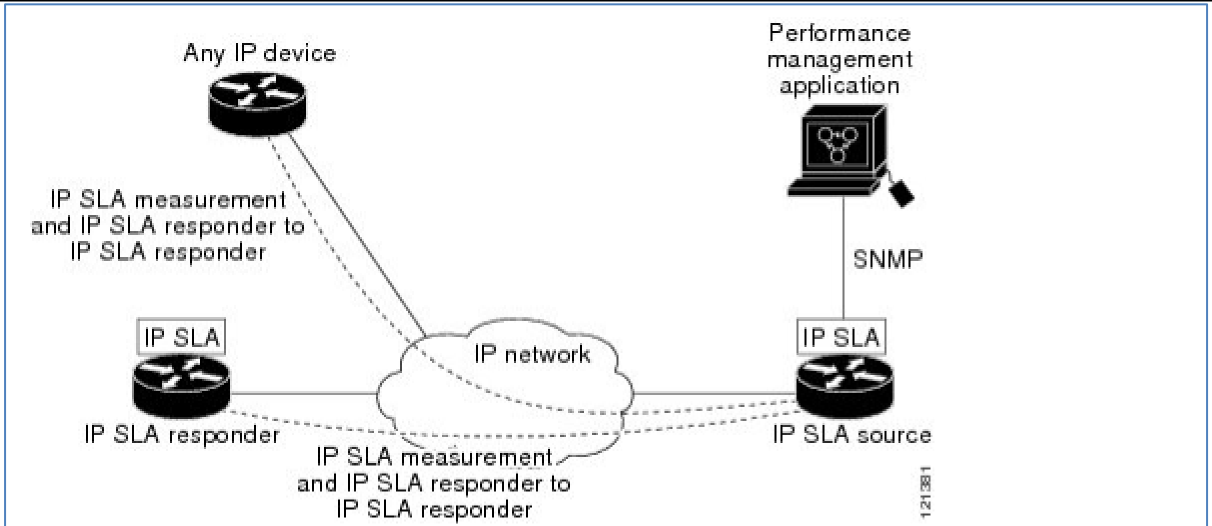
	 *Id.* at 5. The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) through the intermediate network device and back again from the target router to the source router through the intermediate network device. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

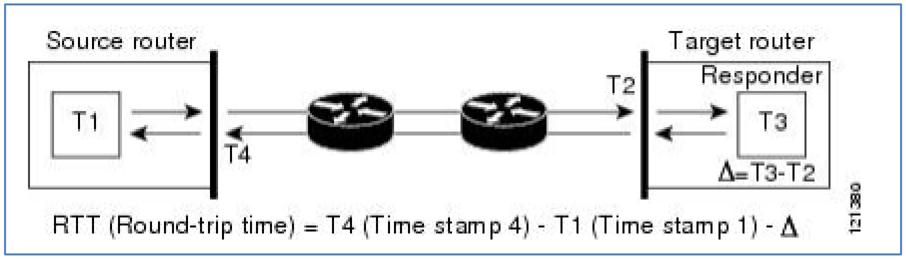
	 *Id.* at 7. "Devices may take tens of milliseconds to process incoming packets, due to other high-priority processes. This delay affects the response times because the reply to test packets might be sitting on queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if IP SLAs Responder is being used), in order to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays." *Id.* at 6. "When a packet arrives at video sink, it is processed to extract the sequence numbers and time stamps, and that information is put into one of the pre-allocated memory blocks. A pointer to this block is put into the used queue for later processing by the main responder task." *Id.* at 75. "At periodic timer intervals, the responder processes a number of the packet information blocks from the used queue and updates the statistics appropriately. When the data is processed, the blocks are returned to the free-memory list to be used again." *Id.* "Having the Receive and Transmit timestamps allows the IP SLA packet to not only measure the RTT of the packet getting from the source to the destination, but also to record how long the destination device takes to process the packet." *IP SLA Fundamentals*, CISCO, https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (last accessed June 20, 2021).
14[D] wherein the message is a loopback message	Cisco Routers and Switches include a loopback message having an uplink path originating from a user element that reaches a network core element and a downlink path returning the loopback message to the user element, as shown below.

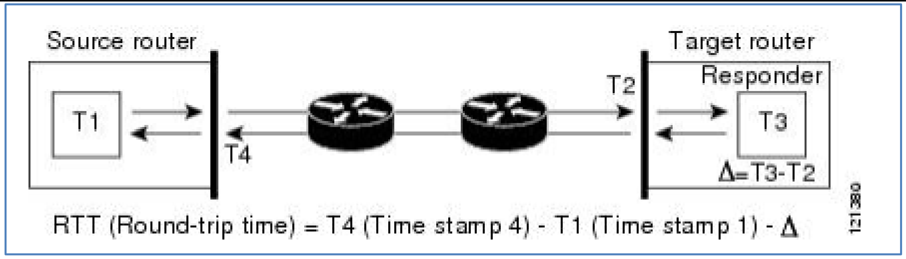
having an uplink path originating from a user element that reaches a network core element and a downlink path returning the loopback message to the user element;	For example, "IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a Cisco router)." *Id.*  *Id.* at 5. The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) through the intermediate network device and back again from the target router to the source router through the intermediate network device. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

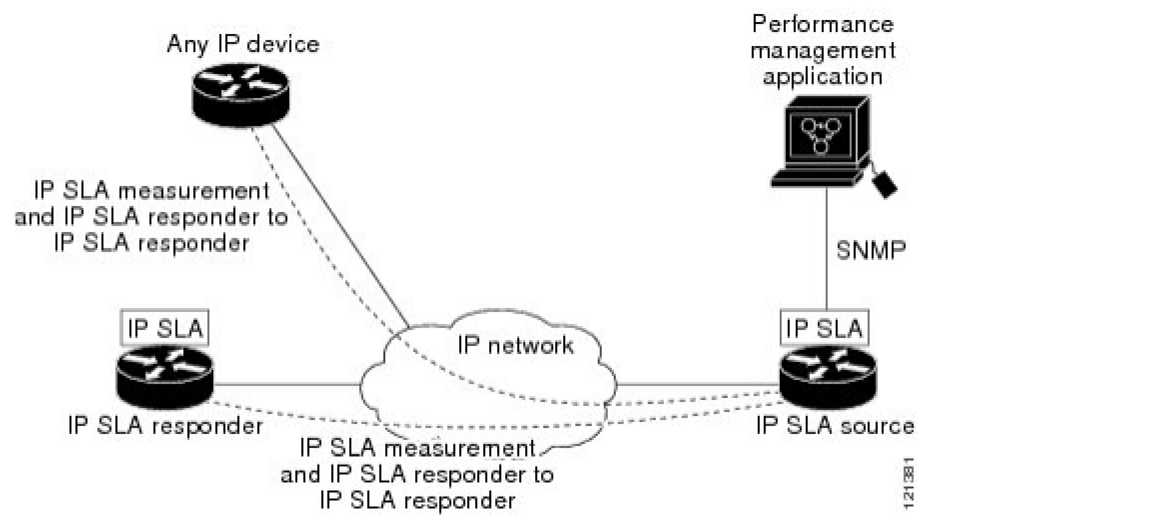
	 *Id.* at 7.
14[E] determine that the message includes the probe session indicator;	Cisco Routers and Switches determine that the message includes the probe session indicator by using time stamping, as shown below. For example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
14[F] based on the message including the probe session indicator:	Cisco Routers and Switches include the probe session indicator generating a first timestamp corresponding to a time of receipt of the message and generating a second timestamp corresponding to a time of transmission of the message, as shown below.

generate a first timestamp corresponding to a time of receipt of the message; generate a second timestamp corresponding to a time of transmission of the message, and	For example, "[w]hen enabled, the IP SLAs Responder allows the target device to take two time stamps both when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time." *Id.* at 6. "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
14[G] transmit the first timestamp and the second timestamp to a first device; and	Cisco Routers and Switches transmit the first timestamp and the second timestamp to a first device (e.g., Network Management System). For example: "SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IP SLAs operations running on the Cisco devices." *Id.* at 2. "After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP." *Id.* at 4–5.

	 To implement IP SLAs network performance measurement you need to perform these tasks: **1** Enable the IP SLAs Responder, if appropriate. **2** Configure the required IP SLAs operation type. **3** Configure any options available for the specified IP SLAs operation type. **4** Configure threshold conditions, if required. **5** Schedule the operation to run, then let the operation run for a period of time to gather statistics. **6** Display and interpret the results of the operation using Cisco software commands or an NMS system with SNMP. *Id.* at 5.
14[H] transmit the message to a second device.	Cisco Routers and Switches transmit the message to a second device (e.g., network elements), as shown below. The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps from sending, processing, to again receiving the processed packet, for example:

	"The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.  *Id.* at 7.
CLAIM 15	
15 The intermediate network device of claim 14, wherein said loopback message traverses the same intermediate nodes on the uplink path and downlink path.	Cisco Routers and Switches include the intermediate network device of claim 14, *see supra* 14[Pre.]-14[H], wherein said loopback message traverses the same intermediate nodes on the uplink path and downlink path. For example, the IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example: "The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

	 *Id.* at 7.
CLAIM 16	
16 The intermediate network device of claim 14, wherein the first device is a network management system.	Cisco Routers and Switches include the intermediate network device of claim 14, *see supra* 14[Pre.]-14[H], wherein the first device is a network management system. For example: "SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs uses the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IP SLAs operations running on the Cisco devices." *Id.* at 2. "After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP." *Id.* at 4–5.

<table>
<tr><td></td><td>


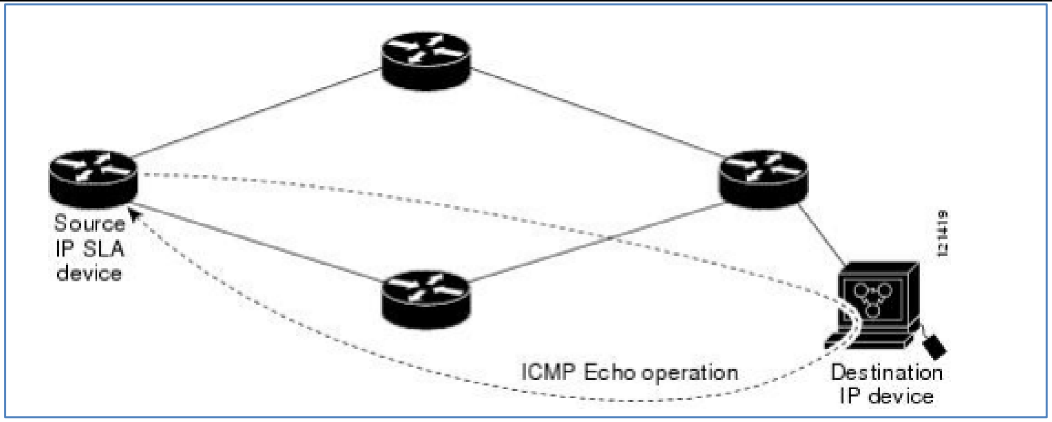
To implement IP SLAs network performance measurement you need to perform these tasks:

1 Enable the IP SLAs Responder, if appropriate.
2 Configure the required IP SLAs operation type.
3 Configure any options available for the specified IP SLAs operation type.
4 Configure threshold conditions, if required.
5 Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6 Display and interpret the results of the operation using Cisco software commands or an NMS system with SNMP.

Id. at 5.
</td></tr>
<tr><td colspan="2">CLAIM 17</td></tr>
<tr><td>17 The intermediate network device</td><td>Cisco Routers and Switches include the intermediate network device of claim 14, see supra 14[Pre.]-14[H], wherein determining that the message includes the probe session indicator is performed by the processor at an application layer of the intermediate network device.</td></tr>
</table>

of claim 14, wherein determining that the message includes the probe session indicator is performed by the processor at an application layer of the intermediate network device.	For example: "Depending on the specific IP SLAs operation, statistics of delay, packet loss, jitter, packet sequence, connectivity, path, server response time, and download time can be monitored within the Cisco device and stored in both CLI and SNMP MIBs. The packets have configurable IP and application layer options such as a source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), a Virtual Private Network (VPN) routing/forwarding instance (VRF), and a URL web address." *Id*. at 2. "Devices may take tens of milliseconds to process incoming packets, due to other high-priority processes. This delay affects the response times because the reply to test packets might be sitting on queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if IP SLAs Responder is being used), in order to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays." *Id.* at 6. "When a packet arrives at video sink, it is processed to extract the sequence numbers and time stamps, and that information is put into one of the pre-allocated memory blocks. A pointer to this block is put into the used queue for later processing by the main responder task." *Id.* at 75. "At periodic timer intervals, the responder processes a number of the packet information blocks from the used queue and updates the statistics appropriately. When the data is processed, the blocks are returned to the free-memory list to be used again." *Id.* "Having the Receive and Transmit timestamps allows the IP SLA packet to not only measure the RTT of the packet getting from the source to the destination, but also to record how long the destination device takes to process the packet." *IP SLA Fundamentals*, CISCO, https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (last accessed June 20, 2021).

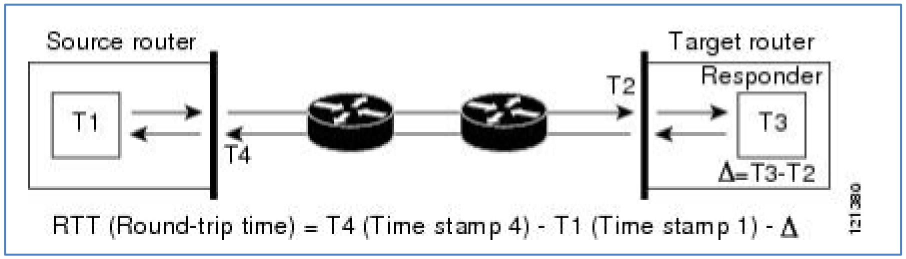
CLAIM 19	
19 The intermediate network device of claim 14, wherein the probe session indicator comprises a probe bit identifying a probe session.	Cisco Routers and Switches include the intermediate network device of claim 14, *see supra* 14[Pre.]-14[H], wherein, on information and belief, the probe session indicator comprises a probe bit identifying a probe session. For example: "The IP SLAs Probe Enhancements feature is an application-aware synthetic operation agent that monitors network performance by measuring response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, for problem analysis, and for designing network topologies." *Id*. at 4.
CLAIM 20	
20 The intermediate network device of claim 14, wherein the message comprises a modified Internet Control Message Protocol (ICMP) PING message.	Cisco Routers and Switches include the intermediate network device of claim 14, *see supra* 14[Pre.]-14[H], wherein the message comprises a modified Internet Control Message Protocol (ICMP) PING message. For example: "In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements." *Id.* at 290.



Id.

The IP SLA test packets use time stamping along a round trip path. A round trip starts with sending an IP SLA packet from the source router (i.e. user element) to the target router (or, core network element) and back again from the target router to the source router. The source and target devices (i.e. network elements) take four timestamps starting from sending, processing to again receiving the processed packet, for example:

"The figure below demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target device, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source device where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy." *Id.* at 6–7.

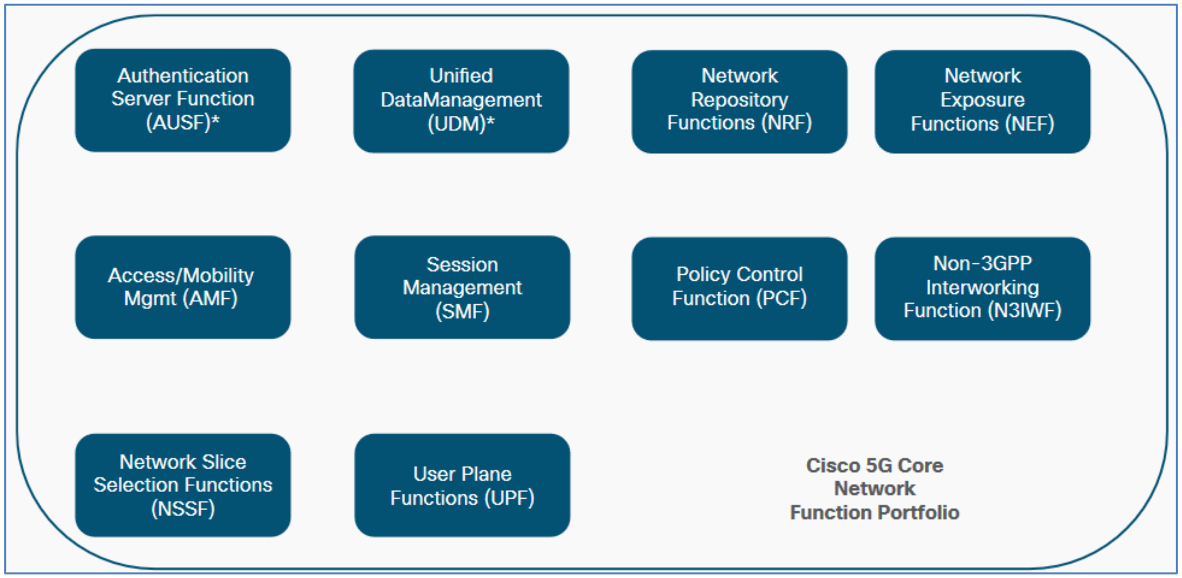


Id. at 7.

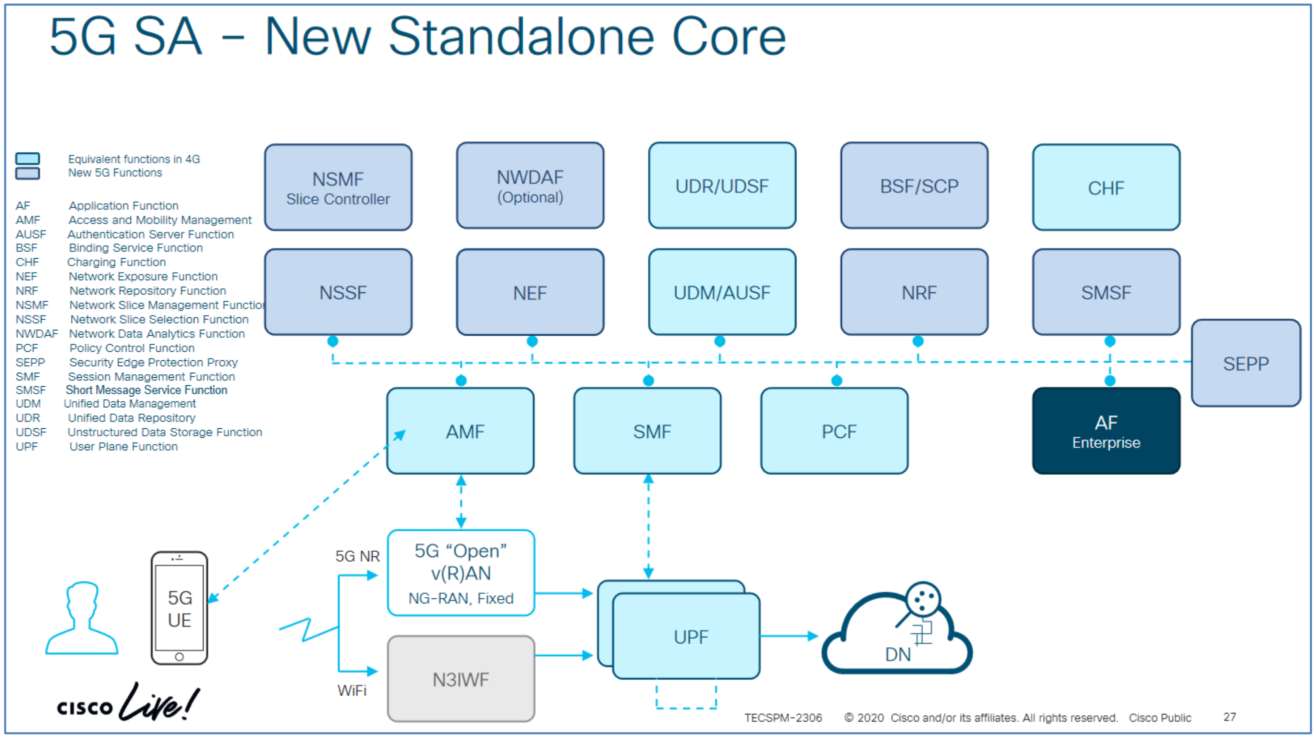
EXHIBIT E

EXHIBIT E

U.S. Patent No. 9,357,014 v. Cisco Ultra Cloud Core and 5G Packet Core Solutions

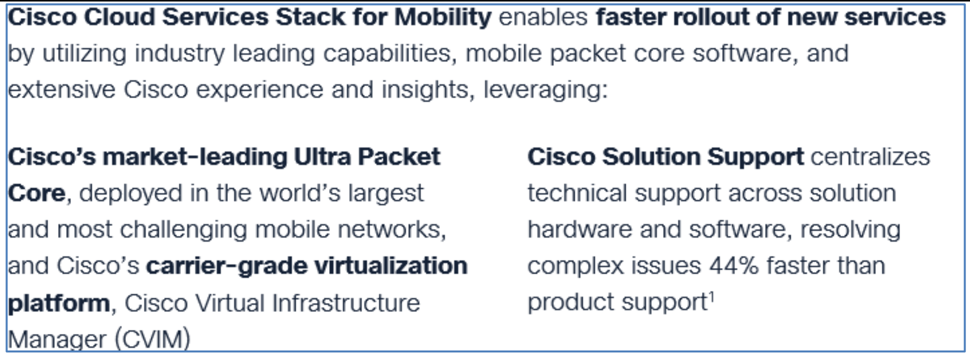
U.S. Patent No. 9,357,014	Application to Cisco Ultra Cloud Core and 5G Packet Core Solutions
CLAIM 1	
1[Pre.] An apparatus, comprising:	To any extent the preamble is limiting, the Cisco Ultra Cloud Core and 5G Packet Core Solutions ("Cisco's Ultra 5G"), including, but not limited to, Cisco Ultra / Virtual Packet Core (VPCSW), are implemented within an apparatus (e.g., Cisco's 500-series routers).  *See* Cisco Ultra 5G Packet Core Solution, CISCO, https://www.cisco.com/c/dam/en/us/products/collateral/routers/network-convergence-system-500-series-routers/white-paper-c11-740360.pdf, at 7-8 (last accessed June 17, 2021).

<table>
<tr>
<td></td>
<td>



See 5G System – Cisco Proposal, CISCO, https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/R6BGArNQ/TECSPM-2306.pdf, at 27 (last accessed June 17, 2021).

</td>
</tr>
<tr>
<td>1[A] a processor and a memory communicatively connected to the processor, the processor configured to run a connected services</td>
<td>Cisco's Ultra 5G consists of an apparatus comprising a processor and a memory communicatively connected to the processor, the processor configured to run a connected services stack, the connected services stack comprising a connected services layer configured to operate below an application layer and above a transport layer.</td>
</tr>
</table>

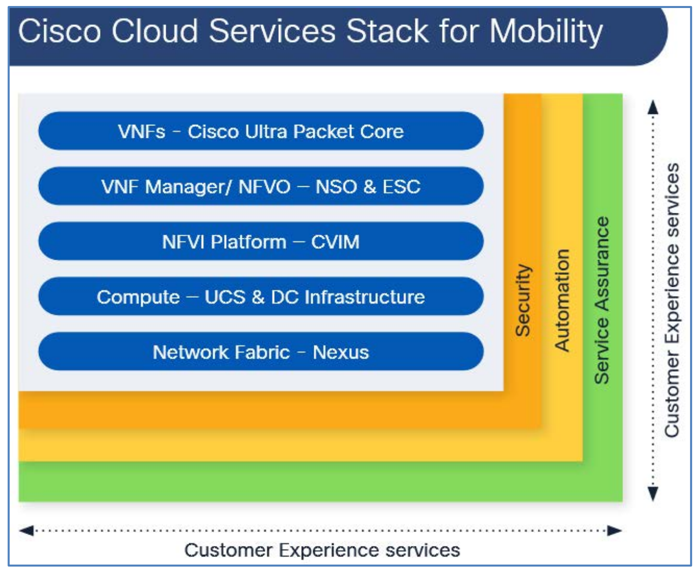
<table>
<tr>
<td>stack, the connected services stack comprising a connected services layer configured to operate below an application layer and above a transport layer, wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint, wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services</td>
<td>


Cisco Cloud Services Stack for Mobility enables **faster rollout of new services** by utilizing industry leading capabilities, mobile packet core software, and extensive Cisco experience and insights, leveraging:

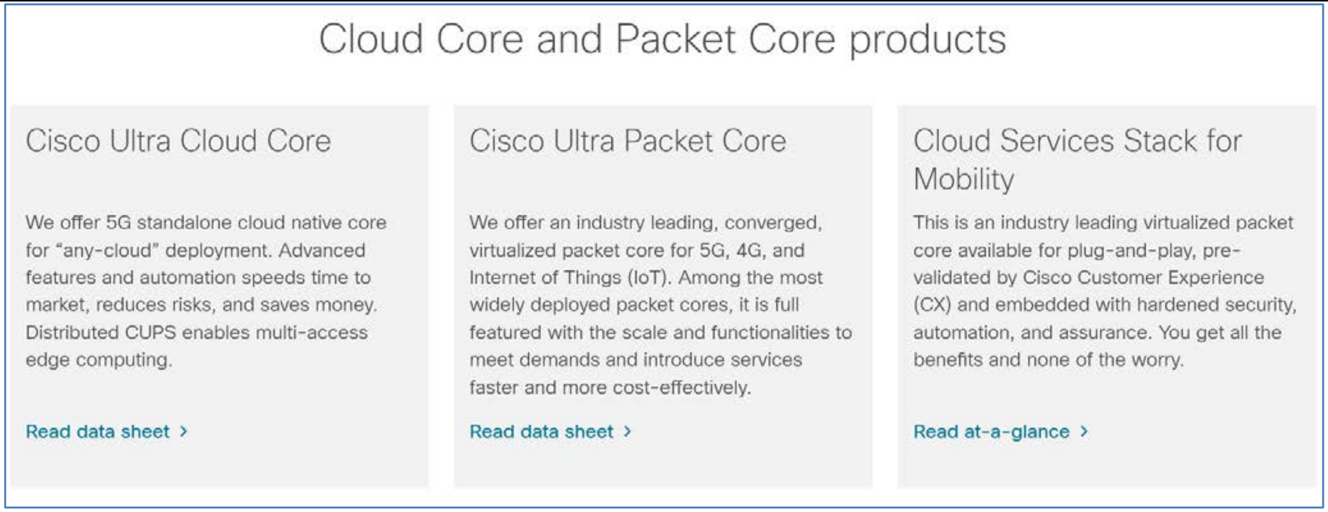
Cisco's market-leading Ultra Packet Core, deployed in the world's largest and most challenging mobile networks, and Cisco's **carrier-grade virtualization platform**, Cisco Virtual Infrastructure Manager (CVIM)

Cisco Solution Support centralizes technical support across solution hardware and software, resolving complex issues 44% faster than product support[1]

See Cisco Cloud Services Stack for Mobility, CISCO, https://www.cisco.com/c/dam/en_us/services/downloads/cisco-cloud-services-stack-mobility-at-a-glance.pdf, at 2 (last accessed June 17, 2021).



See Cisco Cloud Services Stack for Mobility, CISCO, https://www.cisco.com/c/dam/en_us/services/downloads/cisco-cloud-services-stack-mobility-at-a-glance.pdf, at 2 (last accessed June 17, 2021).
</td>
</tr>
</table>

<table>
<tr>
<td>layer, and a service connection identifier for the service connection, wherein the connected services layer is configured to:</td>
<td>


Cloud Core and Packet Core products

Cisco Ultra Cloud Core

We offer 5G standalone cloud native core for "any-cloud" deployment. Advanced features and automation speeds time to market, reduces risks, and saves money. Distributed CUPS enables multi-access edge computing.

Read data sheet ›

Cisco Ultra Packet Core

We offer an industry leading, converged, virtualized packet core for 5G, 4G, and Internet of Things (IoT). Among the most widely deployed packet cores, it is full featured with the scale and functionalities to meet demands and introduce services faster and more cost-effectively.

Read data sheet ›

Cloud Services Stack for Mobility

This is an industry leading virtualized packet core available for plug-and-play, pre-validated by Cisco Customer Experience (CX) and embedded with hardened security, automation, and assurance. You get all the benefits and none of the worry.

Read at-a-glance ›

See Cloud Core and Packet Core Portfolio, CISCO, https://www.cisco.com/c/en/us/products/wireless/packet-core/index.html#~features (last accessed June 17, 2021).

Cisco's Ultra 5G connected services stack offers various network functions (which are performed on at least one processor), such as Access and Mobility Management Functions (AMF), Policy Control Functions (PCF), Session Management Functions (SMF), Network Functions (NF) Repository Functions (NRF), Authentication Server Functions (AUSF), Network Exposure Functions (NEF), etc., which are a part of a connected services layer.

Cisco's 5G SA portfolio is composed of all key mobile core network functions: Access and Mobility management Function (AMF), [[define]] SMF, UPF, PCF, Network Repository Function (NRF), Network Slice Selection Function (NSSF), Network Exposure Function (NEF), Binding Support Function (BSF), Non-3GPP Interworking Function (N3IWF), and Security Edge Protection Proxy (SEPP) (refer to Figure 11).

See Cisco Packet Core 5G Lab Handbook, CISCO, https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSPM-2010-LG.pdf, at 18 (last accessed June 17, 2021).
</td>
</tr>
</table>

Cisco's Ultra 5G further consists of an apparatus wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint.

For example, Cisco's Ultra 5G NF gets a list of NF instances that are registered with the NRF.

> **Nnrf_NFDiscovery**
>
> The Nnrf_NFDiscovery service allows a Network Function Instance to discover services offered by other Network Function Instances, by querying the local NRF.

See Nnrf_NFDiscovery, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/2020-02-0/b_SMF-API-Reference/b_test-SMF_chapter_010010.pdf, at 1 (last accessed June 17, 2021).

Cisco's Ultra 5G further consists of an apparatus wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection.

Cisco's Ultra 5G provides for NF consumers and NF producers to connect with each other by creating sessions to establish service connections (e.g., "the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection").

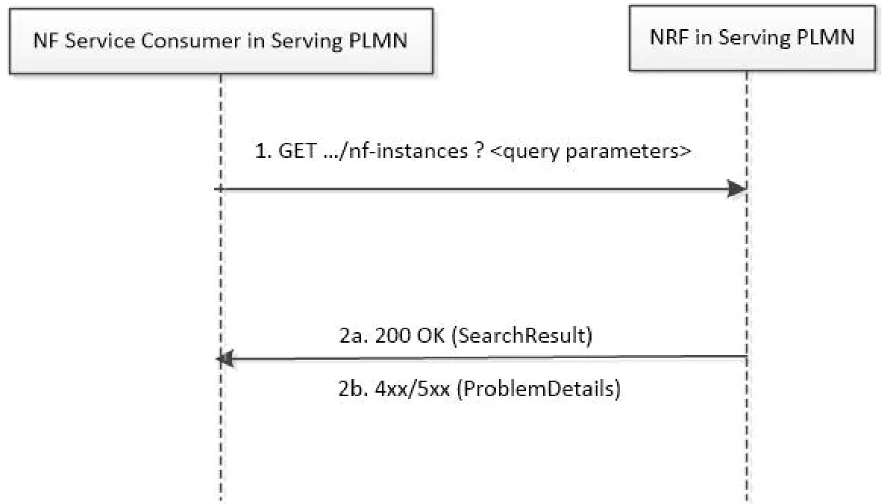
> The three-tiered architecture on which Cisco's CP NFs are designed full support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

See 5G Architecture, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/m_.pdf, 5 (last accessed June 17, 2021).

Cisco's Ultra 5G provides that an NF Consumer that needs to access the services of an NF producer can retrieve the 'NFProfile' of the NF producer by sending, e.g., an HTTP request to the NRF. The HTTP request contains

the NF Instance ID of the consumer (e.g., “service name of the connected services layer”) and the NF instance ID of the Producer (e.g., “service name of the remote connected services layer”).

Figure 2. Service Discovery Request Call Flow



See Ultra Cloud Core 5G Management Function, Release 2020.02, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).

NRF Discovery Support

Based on the 3GPP-defined architecture model for 5G systems for data connectivity, SMF discovers the set of NF instances and their associate NF service instances. These instances, which are based on the NF profiles, are registered in the Network Repository Function (NRF) and meet the various input query parameters.

See id. at 6.

	On success, "200 OK" is returned. The response body contains a validity period, during which the search result can be cached by the NF Service Consumer, and an array of NF profile object that satisfy the search filter criteria (for example, all NF Instances offering a certain NF Service name). *See id*. at 4. The NF 'serviceName' along with the 'version' act (e.g., "the service connection identifier") provide connection identification between the NF consumer and the NF producer. 6.5 NF Service Instance Reselection If a formerly selected NF Service Instance becomes unavailable, the NF Service Consumer may select a different instance of a same NF Service, in the same NF Instance, if the NF Instance indicates in its NF Profile that it supports the capability to persist their resources in shared storage inside the NF Instance, and if the new NF Service Instance offers the same major service version. *See* 5G System Restoration Procedures, ETSI, https://www.etsi.org/deliver/etsi_ts/123500_123599/123527/15.03.00_60/ts_123527v150300p.pdf, at 19 (last accessed June 17, 2021). Further, Cisco's Ultra 5G practices said method wherein the connected services layer is configurable.

	Features and benefits Table 1. Ultra Cloud Core features and benefits (see table below)

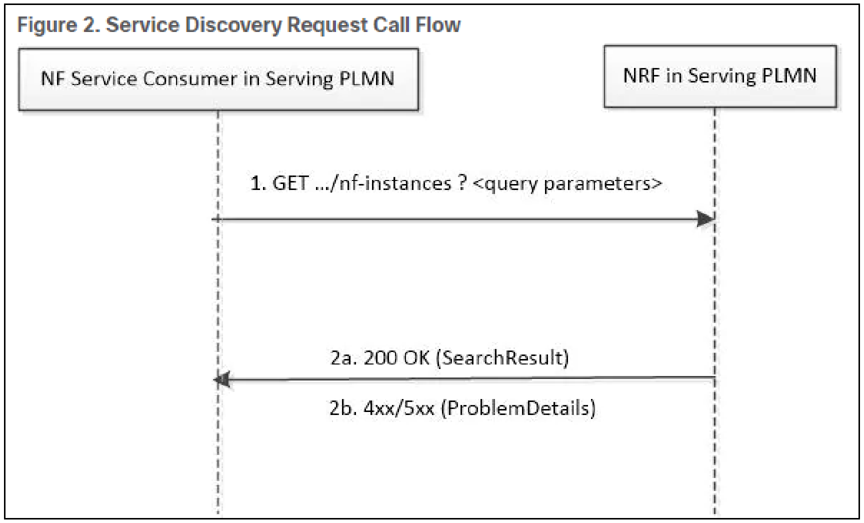
Features and benefits

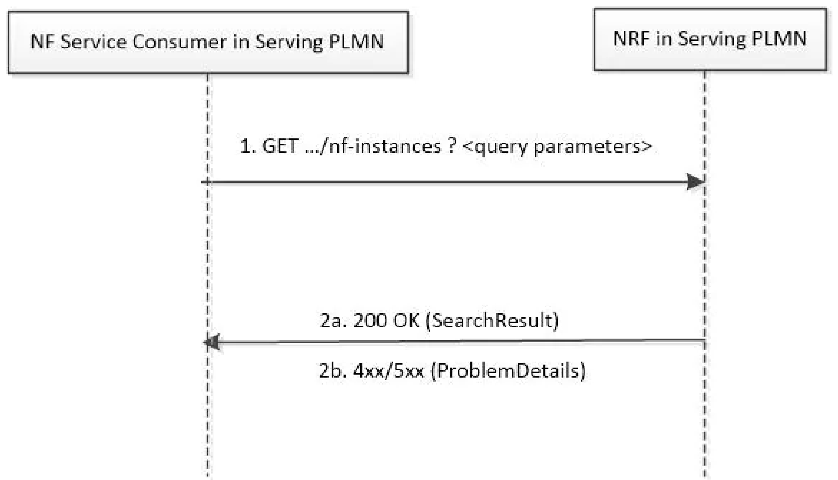
Table 1. Ultra Cloud Core features and benefits

Feature	Benefit
Cisco intelligent service mesh	What it is: Intelligent service mesh routes traffic within the cluster to specific application instances. Result: Multiple variations and configurations of services can run concurrently. Result: New services and upgrades can be introduced with very low risk.
Common execution environment	What it is: Common components for logging, alarming, events, deployment, upgrades, configuration, and provisioning Result: Cisco 5G applications are configured the same, deployed the same, and share the same logging, alarming, telemetry components. Result: Onboarding additional Cisco applications is easy.
Cisco operations center	What it is: An agent can deploy applications using a YANG schema and expose NETCONF/RESTCONF interfaces to each product by integrating with Cisco Network Services Orchestrator. Result: Common API, command line interface (CLI), and GUI interface to each 5G application Result: All change management can be orchestrated.
Granular tracing	What it is: Integration with application dynamics and open tracing for traffic flow monitoring Result: A new level of visibility of traffic flows across network functions and between and within services
Release automation framework	What it is: This framework provides the ability to automate testing as part of the service deployment. Result: Testing becomes part of the service deployment workflow. Result: This automation reduces the time needed to certify new services, code, and new configurations, and reduces the time to market.

See Cisco Ultra Cloud Core Data Sheet, https://www.cisco.com/c/en/us/products/collateral/wireless/packet-core/datasheet-c78-744630.html (last accessed June 17, 2021) (noting various Cisco Ultra 5G elements which are configurable).

Thus, Cisco's Ultra 5G consists of an apparatus comprising a processor and a memory communicatively connected to the processor, the processor configured to run a connected services stack, the connected services

	stack comprising a connected services layer configured to operate below an application layer and above a transport layer, wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint, wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection, wherein the connected services layer is configured.
1[B] send, toward a server, a service connection request message comprising the service name of the connected services layer and the service name of the remote connected services layer of the remote endpoint; and	Cisco's Ultra 5G consists of an apparatus which sends, towards a server, a service connection request message comprising the service name of the connected services layer and the service name of the remote connected services layer of the remote endpoint. In Cisco's Ultra 5G, an NF Consumer can retrieve the NFProfile of an NF producer by sending a HTTP request to the NRF (e.g., "a server") containing an identifier of the consumer (e.g., "a service connection request message comprising the service name of the connected services layer") and an identifier of the NF Producer (e.g., "...and the service name of the remote connected services layer of the remote endpoint").  *See* Ultra Cloud Core 5G Management Function, Release 2020.02, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).

1[C] receive, from the server, a service connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection.	Cisco's Ultra 5G consists of an apparatus which receives, from the server, a service connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection. The NRF (e.g., "a server") receives the HTTP request and responds with an HTTP message containing an identifier that includes a Producer's NF instanceID, IP address, the service name, and the version (e.g., "a service connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection") for the connection. Figure 2. Service Discovery Request Call Flow  *See* Ultra Cloud Core 5G Management Function, Release 2020.02, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).

NFProfile

Type: object

Required:

- nfInstanceId

- nfType

- nfStatus

See Nnrf_NFDiscovery, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/2020-02-0/b_SMF-API-Reference/b_test-SMF_chapter_010010.pdf, at 10 (last accessed June 17, 2021).

ipv4Addresses:

Type: array

Items:

Reference: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'

minItems: 1

ipv6Addresses:

Type: array

See id. at 11.

nfServices:

Type: array

Items:

Reference: '#/components/schemas/NFService'

See id. at 12.

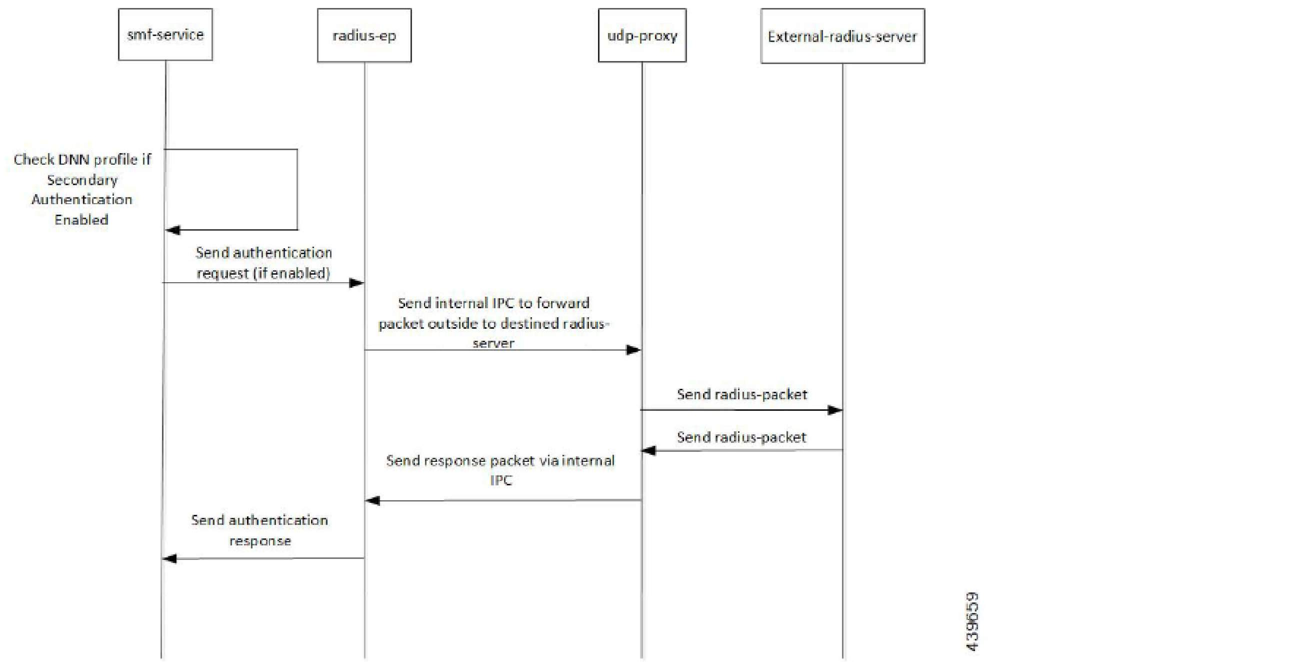
	NFService **Type**: object **Required**: - serviceInstanceId - serviceName - versions - scheme - nfServiceStatus *See id*. at 13.
CLAIM 2	
2[A] The apparatus of claim 1, wherein the service connection response message further comprises one or more encryption keys for the service connection.	Cisco's Ultra 5G consists of an apparatus which comprises a service connection response message further comprises one or more encryption keys for the service connection. *See* 1[A], *supra*. With the X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, you can append headers to HTTP or WSP GET and POST request packets, and HTTP response packets for use by end applications. For example, mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on. *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 181 (last accessed June 17, 2021).

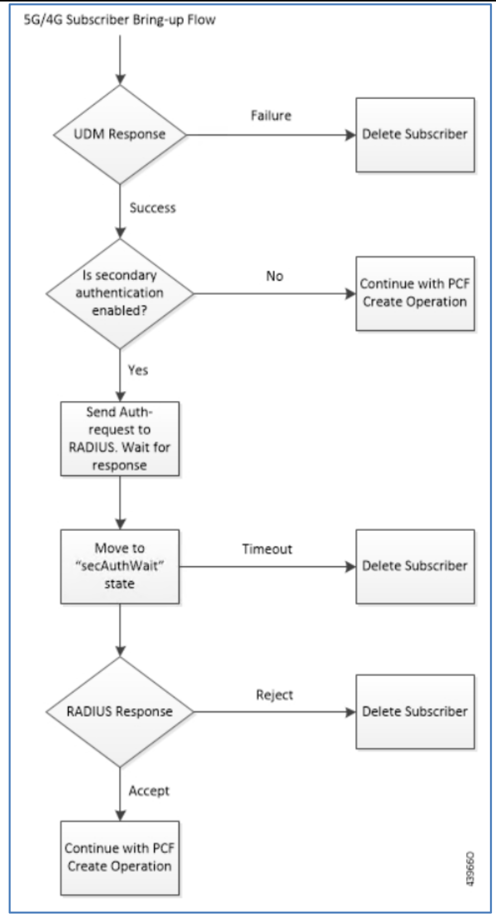
<table>
<tr><td></td><td>

```
configure
   active-charging service acs_service_name
      charging-action charging_action_name
         xheader-insert xheader-format xheader_format_name [ encryption {
rc4md5 | aes-256-gcm-sha384 [ salt ] } [ encrypted ] key key ] [
first-request-only ] [ msg-type { response-only | request-and-response }
 ] [ -noconfirm ]
         end
```

See id. at 185.</td></tr>
<tr><td colspan="2">CLAIM 3</td></tr>
<tr><td>3[A] The apparatus of claim 1, wherein the connected services layer is configured to send the service connection request message responsive to:</td><td>Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configured to send a service connection request message. See 1[A], supra.</td></tr>
<tr><td>3[B] a communication request from an application via the application layer; or a determination that an application is expected to request communication via the application layer.</td><td>Cisco's Ultra 5G sends the service connection request message responsive to a communication request from an application via the application layer; or a determination that an application is expected to request communication via the application layer.

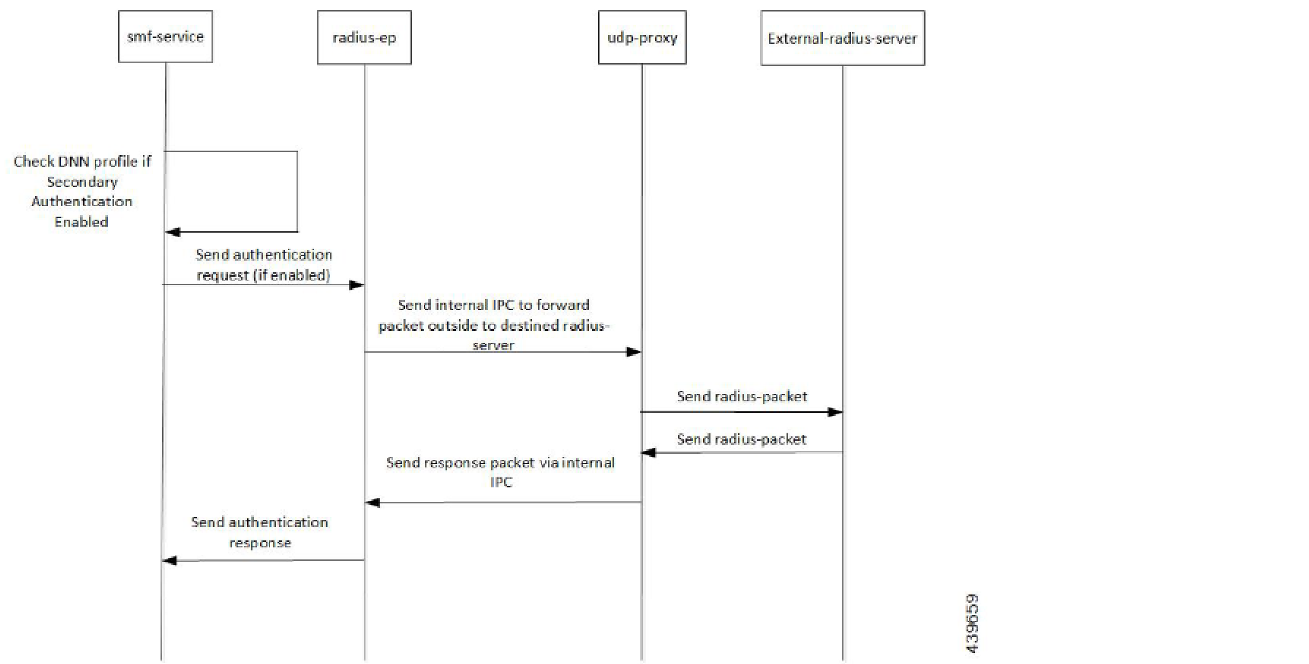
As one non-limiting example, Cisco's Ultra 5G smf-service sends an authentication request to the radius-ep and, in response, receives an authentication response from the radius-ep at the smf-service (e.g., "a communication request from an application via the application layer; or a determination that an application is expected to request communication via the application layer").</td></tr>
</table>

	The following figure illustrates the end to end call flow between SMF server and RADIUS-EP functionality.  *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 511 (last accessed June 17, 2021).

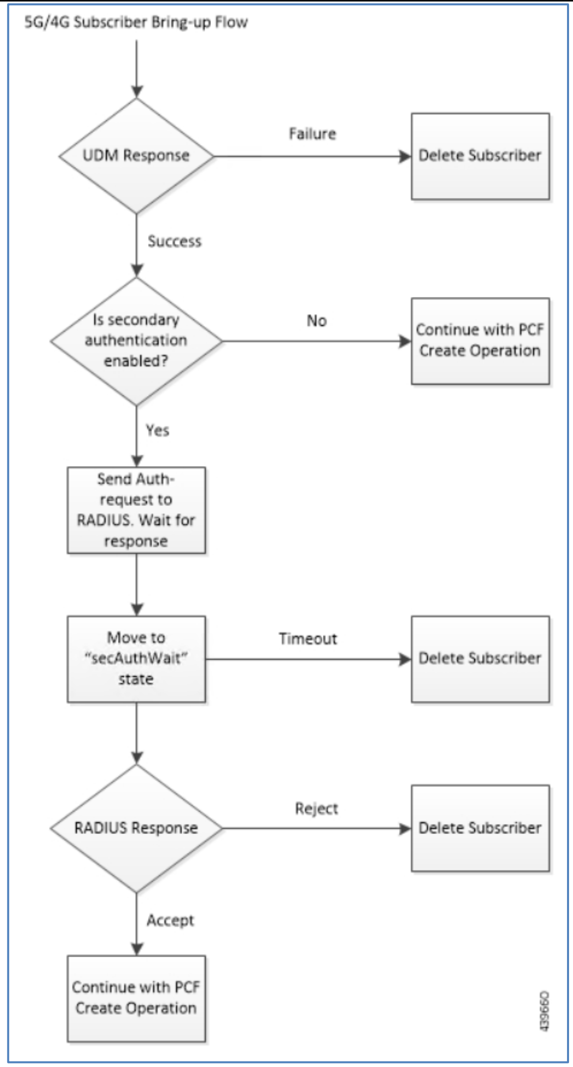
	 *See id.* at 512-13.
CLAIM 4	
4[A] The apparatus of claim 1, wherein the connected services layer is	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configured to maintain authentication information configured for use by the connected services layer in authenticating with the server.

<table>
<tr>
<td>configured to maintain authentication information configured for use by the connected services layer in authenticating with the server.</td>
<td>
As one non-limiting example, the smf-service sends authentication requests and expects an authentication response to maintain authentication.

The following figure illustrates the end to end call flow between SMF server and RADIUS-EP functionality.

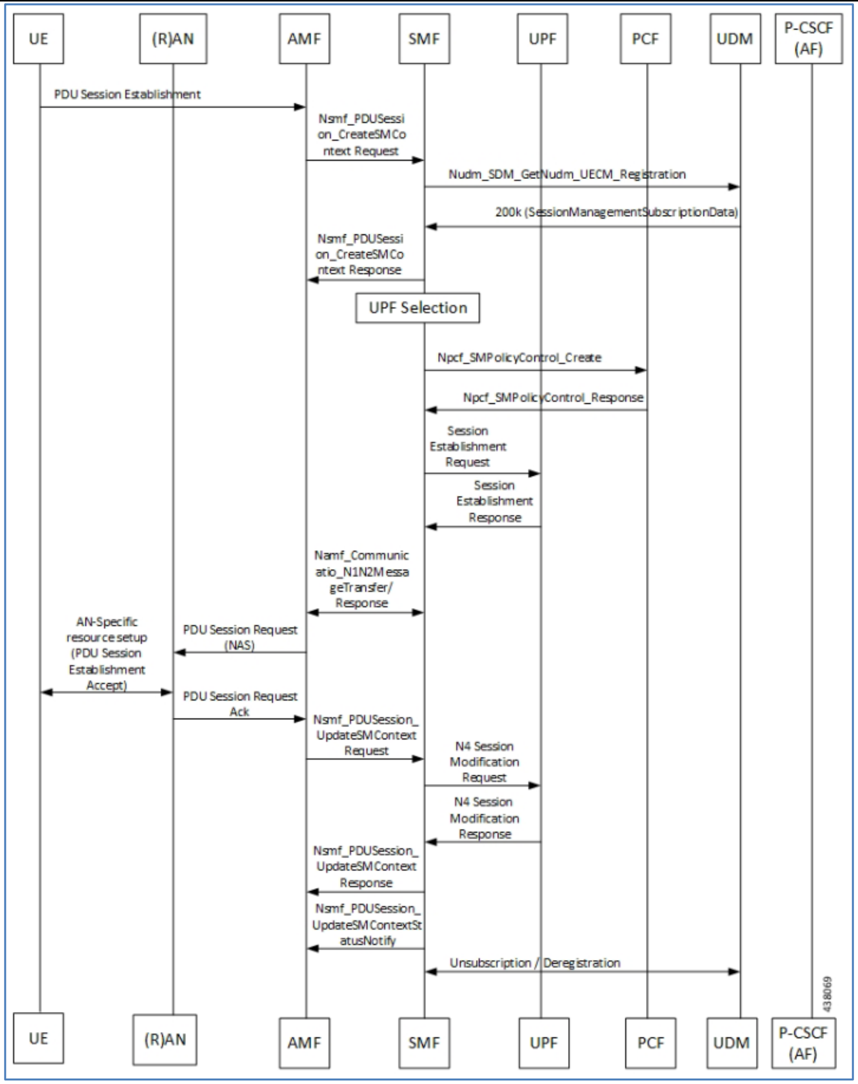


See Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 511 (last accessed June 17, 2021).
</td>
</tr>
</table>

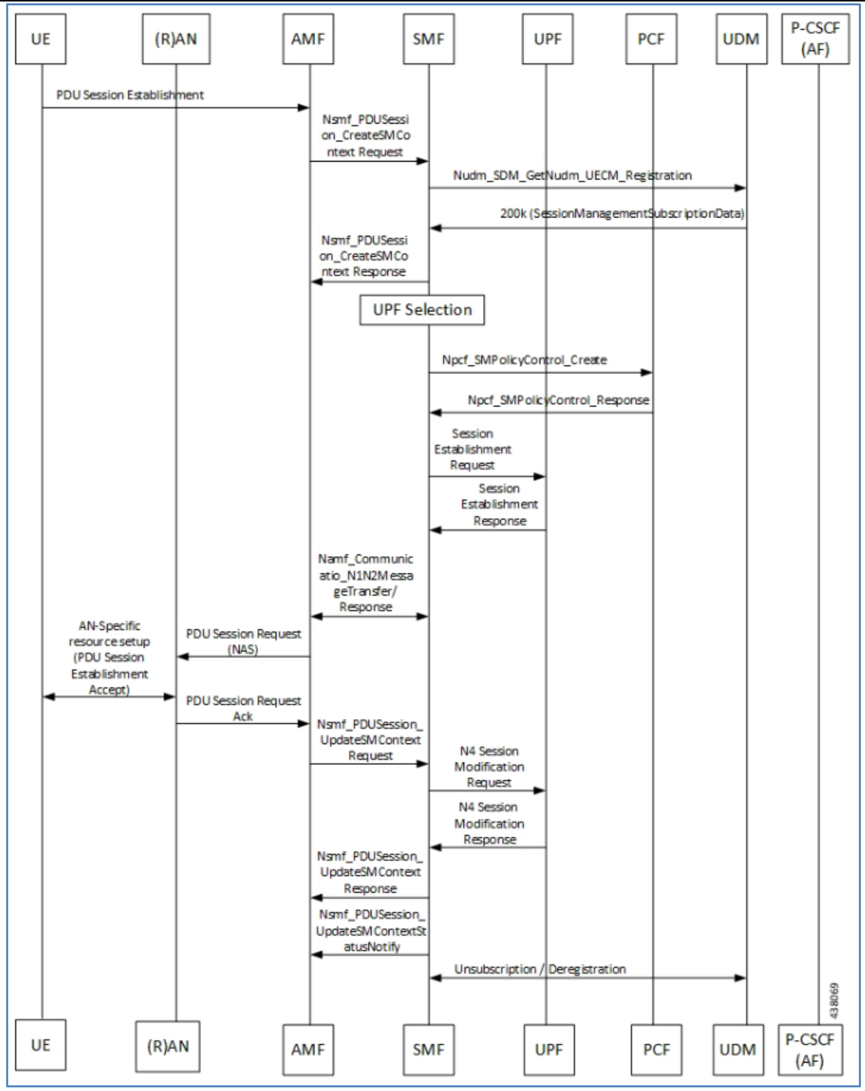


See id. at 512-13 (“After successful UDM Subscriber-Notification response, smf-service invokes secondary authentication if enabled in the DNN-profile configuration.”).

CLAIM 5	
5[A] The apparatus of claim 1, wherein the connected services layer is configured to:	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. *See* 1[A], *supra*.
5[B] maintain a set of service connection information for the service connection, the set of service connection information comprising the service connection identifier for the service connection, the service name of the remote connected services layer of the remote endpoint, and the IP address of the remote endpoint.	Cisco's Ultra 5G consists of an apparatus which maintains a set of service connection information for the service connection, the set of service connection information comprising the service connection identifier for the service connection, the service name of the remote connected services layer of the remote endpoint, and the IP address of the remote endpoint. As one non-limiting example, the SMF creates a request that is sent to the User Plane Function (UPF) which contains IP addresses and/or prefixes. This implies that the SMF maintains such service connection information as is necessary to at least form and send such a request.

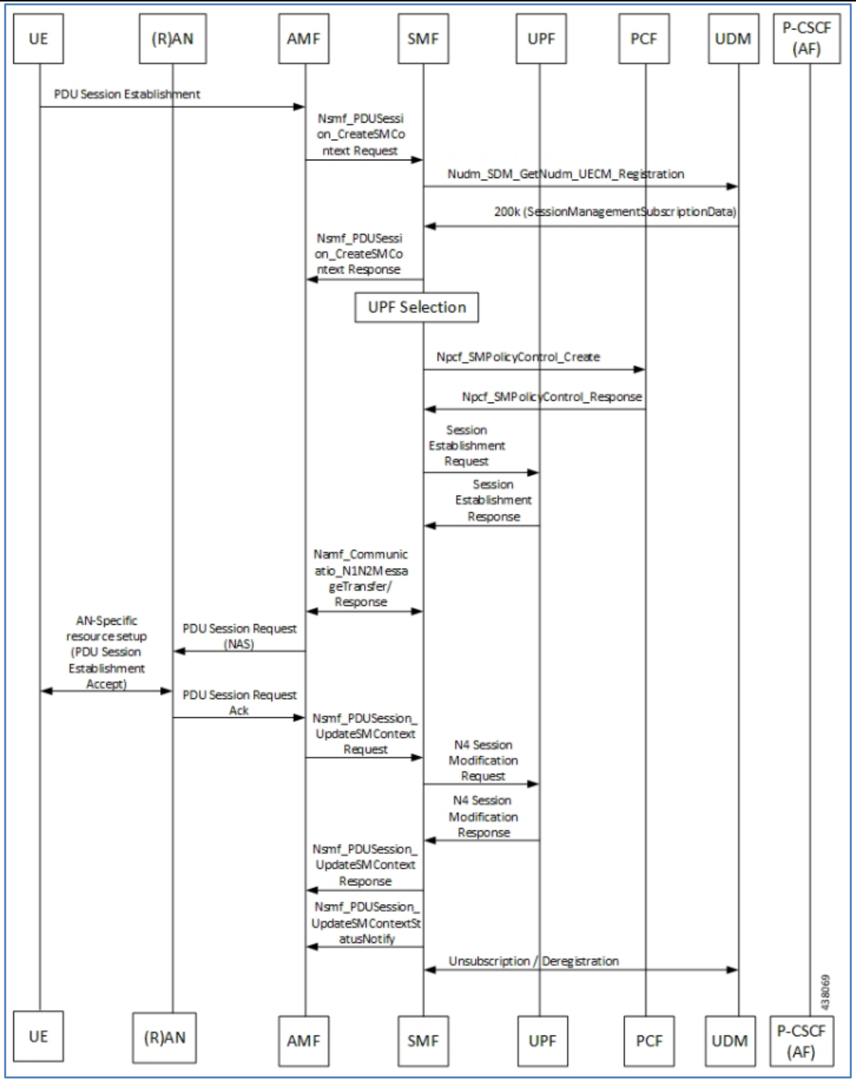
	 *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 601 (last accessed June 17, 2021).

	The SMF initiates "Npcf_SMPolicyControl_Create" Request by including "SmPolicyContextData", which contains Supi, pduSessionId, ratType, servingNetwork, userLocationInfo, ueTimeZone, Pei, Online/Offline charging, chargingcharacteristics, PDU Session-Type, allocated UE IP address/prefix(es), subsDefQos, and information. *See id*. at 602.
CLAIM 6	
6[A] The apparatus of claim 1, wherein the connected services layer is configured to:	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. *See* 1[A], *supra*.
6[B] initiate establishment of the service connection with the remote connected services layer of the remote endpoint by propagating, toward the remote connected services layer of the remote endpoint, a service connection establishment request message comprising the service connection identifier for the	Cisco's Ultra 5G consists of an apparatus which initiates establishment of the service connection with the remote connected services layer of the remote endpoint by propagating, toward the remote connected services layer of the remote endpoint, a service connection establishment request message comprising the service connection identifier for the service connection and the IP address of the remote endpoint. As one non-limiting example, the SMF creates a request that is sent to the User Plane Function (UPF) which contains the IP address allocated to a UE.

<table>
<tr>
<td>service connection and the IP address of the remote endpoint.</td>
<td>


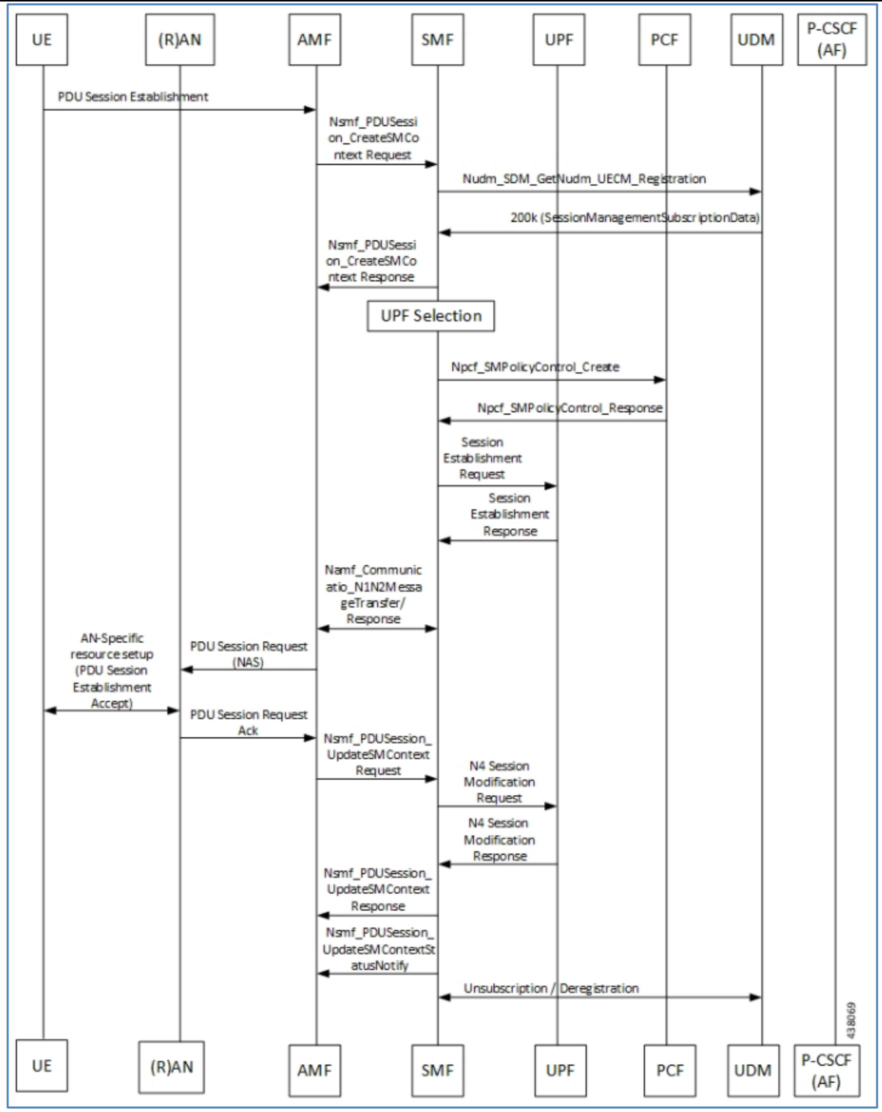
See Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 601 (last accessed June 17, 2021).
</td>
</tr>
</table>

	The SMF initiates "Npcf_SMPolicyControl_Create" Request by including "SmPolicyContextData", which contains Supi, pduSessionId, ratType, servingNetwork, userLocationInfo, ueTimeZone, Pei, Online/Offline charging, chargingcharacteristics, PDU Session-Type, allocated UE IP address/prefix(es), subsDefQos, and information. *See id*. at 602.
CLAIM 7	
7[A] The apparatus of claim 6, wherein the connected services layer is configured to:	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. *See* 6[A], *supra*.
7[B] participate in a handshake with the remote connected services layer of the remote endpoint for establishing the service connection with the remote connected services layer of the remote endpoint.	Cisco's Ultra 5G consists of an apparatus which participates in a handshake with the remote connected services layer of the remote endpoint for establishing the service connection with the remote connected services layer of the remote endpoint. As one non-limiting example, the SMF creates a session establishment request that is sent to the User Plane Function (UPF). The UPF then returns a session establishment response to the SMF.

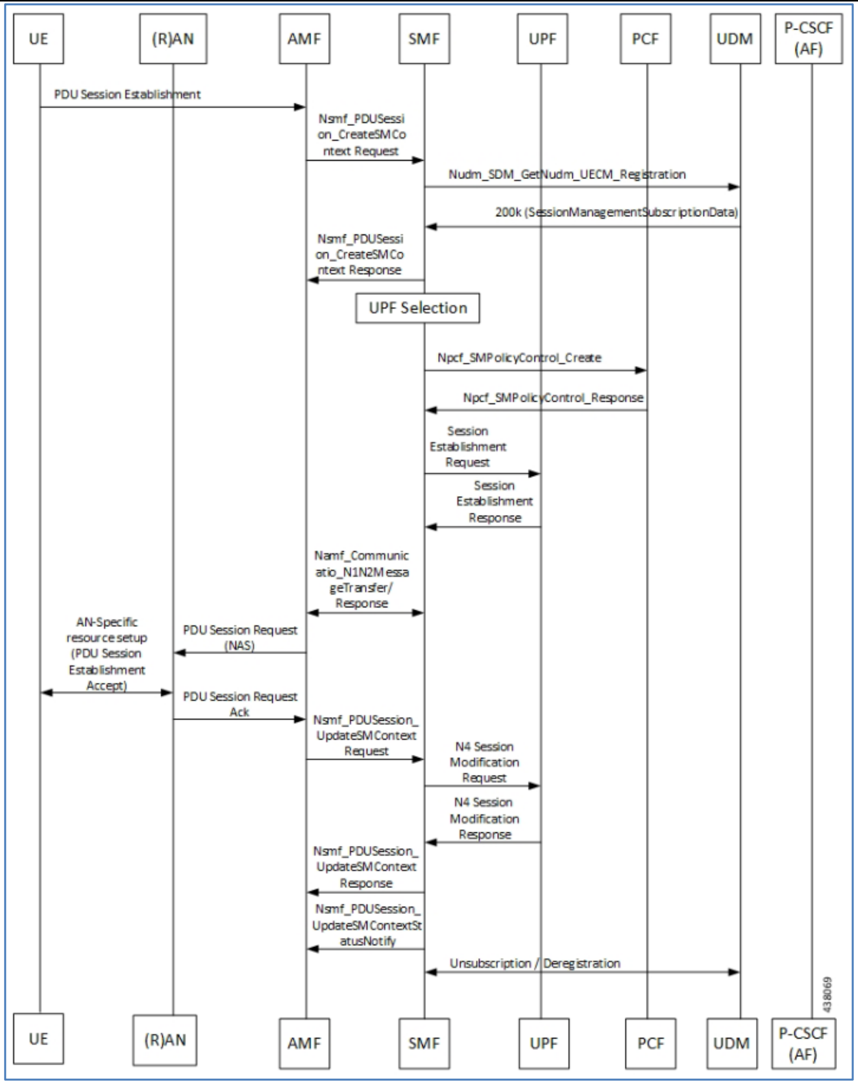


See Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 601 (last accessed June 17, 2021).

	The PCF responds back with "Npcf_SMPolicyControl_CreateResponse (200 OK)" by including "SmPolicyDecision" in the message to the SMF. "SmPolicyDecision" contains the sessionRules, pccRules, qosDecs, chgDecs, chargingInfo, traffConDecs, umDecs, qosChars, and so on as defined in the 3GPP TS 29.512, Section 5.6.2.4. All these parameters are only applicable for "IMS Voice over PS session". This section does not cover Data and Voice PDU sessions. **Note** When a UE initiates a Resource Modification Request, and if the SMF includes the "qosFlowUsage" attribute containing "IMS_SIG" within SmPolicyUpdateContextDatadata structure and the PCF accepts that a QoS flow dedicated to IMS signaling can be used, the PCF returns the "qosFlowUsage" containing "IMS_SIG" value within the SmPolicyDecision data structure. The PCC rules provided have the 5QI applicable for IMS signaling. *See id.* at 602.
CLAIM 8	
8[A] The apparatus of claim 6, wherein the connected services layer is configured to:	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. *See* 6[A], *supra*.
8[B] negotiate a set of service connection parameters with the remote connected services layer of the remote endpoint during establishment of the	Cisco's Ultra 5G consists of an apparatus which negotiates a set of service connection parameters with the remote connected services layer of the remote endpoint during establishment of the service connection with the remote connected services layer of the remote endpoint. As one non-limiting example, the SMF establishment request negotiates subsDefQos and ueTimeZone (e.g., "service connection parameters").

service connection with the remote connected services layer of the remote endpoint.	 *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 601 (last accessed June 17, 2021).

	The SMF initiates "Npcf_SMPolicyControl_Create" Request by including "SmPolicyContextData", which contains Supi, pduSessionId, ratType, servingNetwork, userLocationInfo, ueTimeZone, Pei, Online/Offline charging, chargingcharacteristics, PDU Session-Type, allocated UE IP address/prefix(es), subsDefQos, and information. *See id*. at 602.
CLAIM 9	
9[A] The apparatus of claim 1, wherein the connected services layer is configured to:	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. *See* 1[A], *supra*.
9[B] establish the service connection with the remote connected services layer of the remote endpoint based on the service connection identifier for the service connection and the IP address of the remote endpoint.	Cisco's Ultra 5G consists of an apparatus which establishes the service connection with the remote connected services layer of the remote endpoint based on the service connection identifier for the service connection and the IP address of the remote endpoint. As one non-limiting example, the UPF sends an SessionEstablishmentResponse during session creation call flow.

	 *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 601 (last accessed June 17, 2021).

<table>
<tr><td></td><td>

> The SMF initiates "Npcf_SMPolicyControl_Create" Request by including "SmPolicyContextData", which contains Supi, pduSessionId, ratType, servingNetwork, userLocationInfo, ueTimeZone, Pei, Online/Offline charging, chargingcharacteristics, PDU Session-Type, allocated UE IP address/prefix(es), subsDefQos, and information.

See id. at 602.

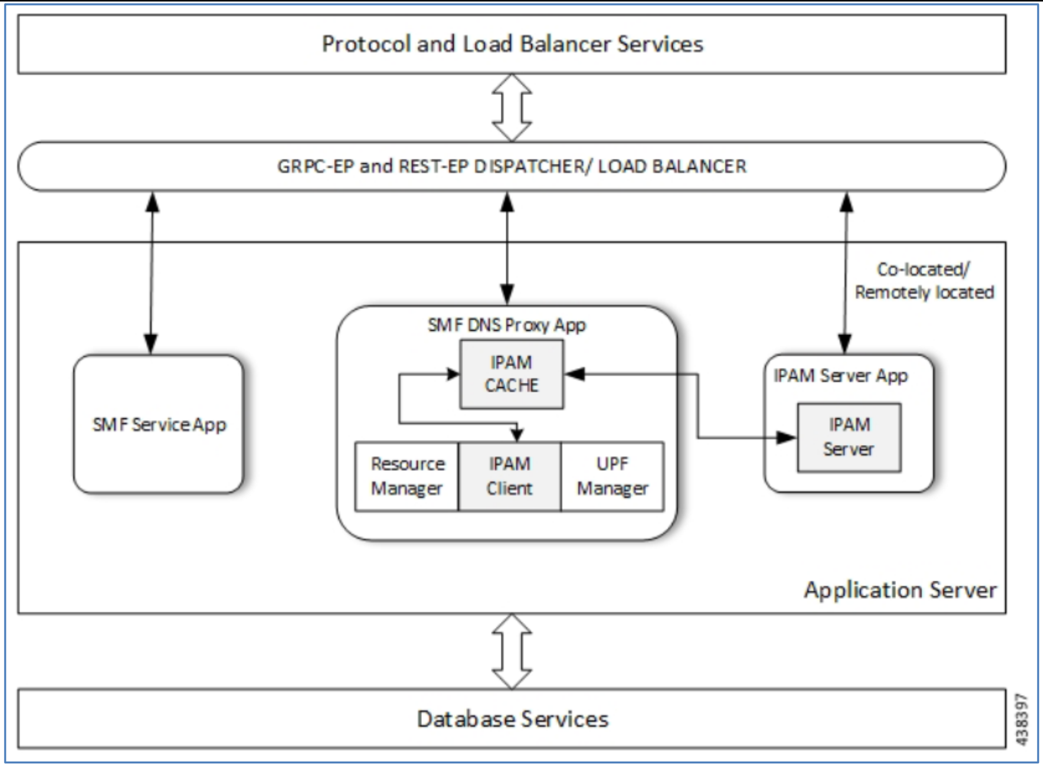
> The UPF acknowledges by sending an N4 Session Establishment Response. If CN Tunnel Info is allocated by the UPF, the CN Tunnel Info is provided to SMF in this step.

See id. at 603.</td></tr>
<tr><td colspan="2">CLAIM 12</td></tr>
<tr><td>12[A] The apparatus of claim 1, wherein the connected services layer is configured to:</td><td>Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. See 1[A], supra.</td></tr>
<tr><td>12[B] based on a change of the apparatus from the IP address to a new IP address:</td><td>Cisco's Ultra 5G performs a function based on a change of the apparatus from the IP address to a new IP address.

As one non-limiting example, the SMF utilizes the IP Address Management technique for managing IP addresses.

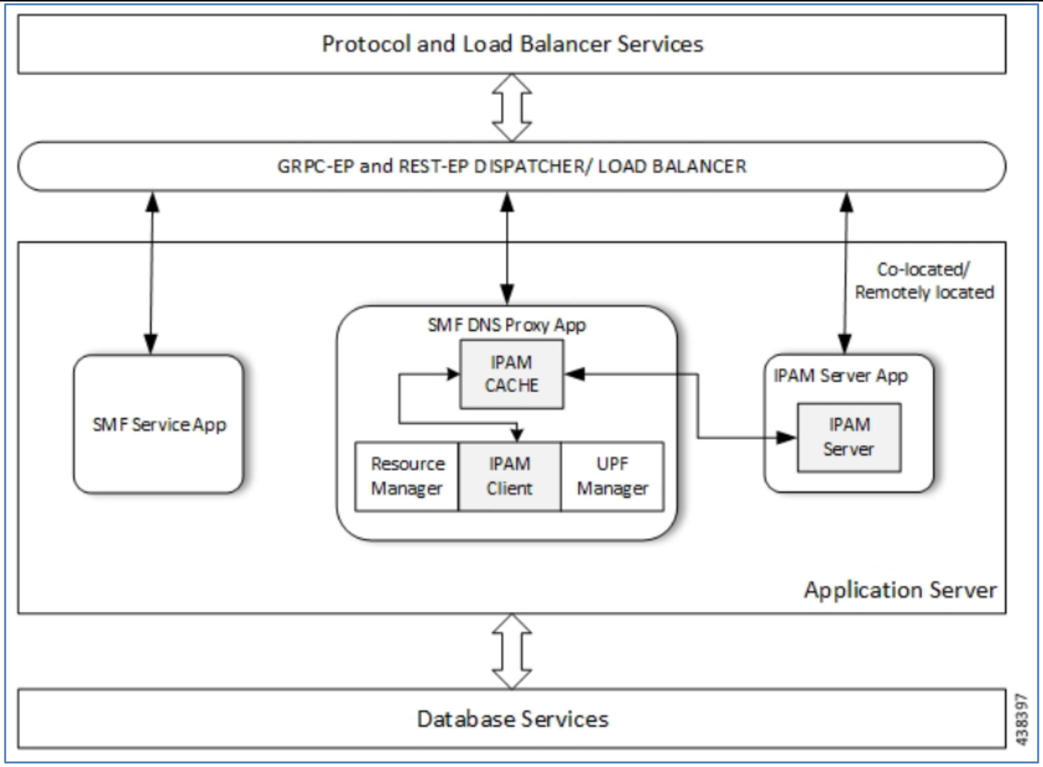
> IP Address Management (IPAM) is a technique for tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. The IPAM provides all the functionalities necessary for working with the cloud-native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the Session Management Function (SMF), Policy Control Function (PCF), and so on.</td></tr>
</table>

	See Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 11 (last accessed June 17, 2021).
12[C] propagate, toward the server, an IP address change notification message including the service connection identifier for the service connection and the new IP address of the apparatus.	Cisco's Ultra 5G propagates, toward the server, an IP address change notification message including the service connection identifier for the service connection and the new IP address of the apparatus. As one non-limiting example, Cisco's Ultra 5G through the SMF and IPAM handle IP address propagation (e.g., requests and releases) during session establishment and termination. The IPAM cache, client, and server manage address change notifications during this session establishment and termination process, including for new IP addresses. • **SMF Node-Manager Application** – The SMF Node-Manager application takes care of the UPF, ID resource, and IP address management. Therefore, the SMF Node-Manager application integrates IPAM Cache and IPAM client modules. The UPF Manager uses the IPAM Client module for address-range-reservation per UPF. • **SMF Service Application** – The SMF Service application provides PDU session services. During session establishment and termination, the IP addresses are requested and released back. The SMF Service application invokes the IPC to RMGR in Node Manager, which receives (free) the IP from the IPAM module. • **IPAM Server Application** – Based on the deployment model, the IPAM Server application can run as an independent microservice, as a part of the same cluster, or in a remote-cluster. For standalone deployments, the IPAM Servers are an integral part of the IPAM cache. *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 312 (last accessed June 17, 2021).

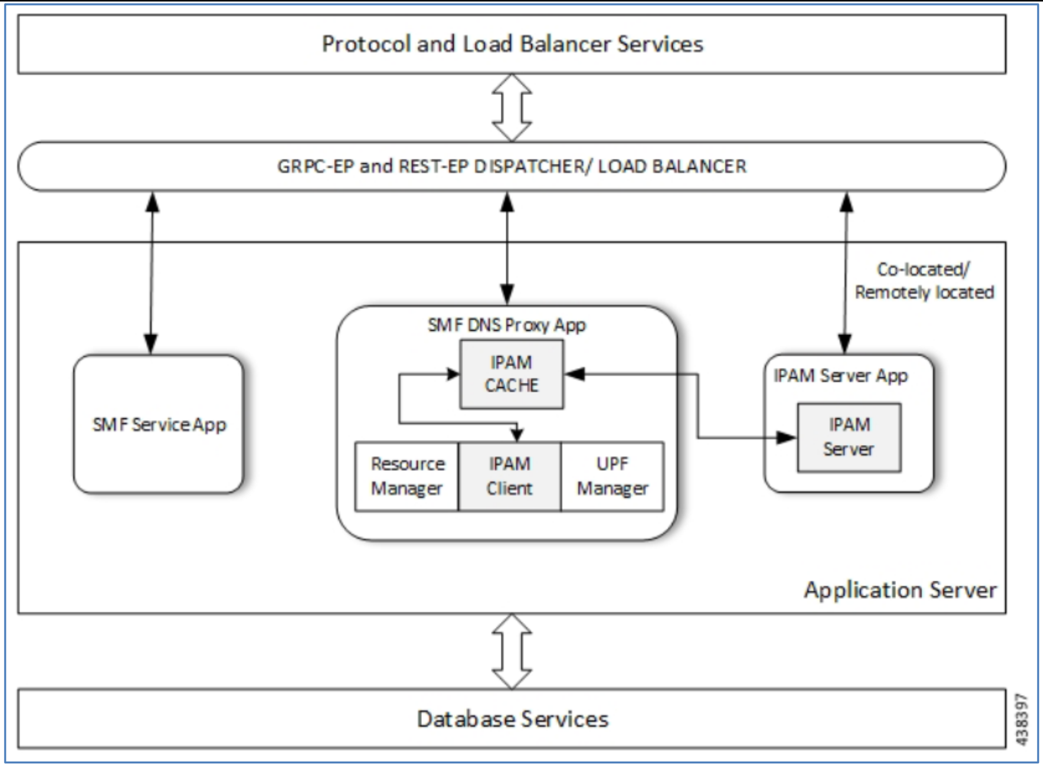
	 *See id.*
CLAIM 13	
13[A] The apparatus of claim 1, wherein the connected services layer is configured to:	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configurable. *See* 1[A], *supra*.

13[B] based on a change of the apparatus from the IP address to a new IP address:	Cisco's Ultra 5G performs a function based on a change of the apparatus from the IP address to a new IP address. As one non-limiting example, the SMF utilizes the IP Address Management technique for managing IP addresses. IP Address Management (IPAM) is a technique for tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. The IPAM provides all the functionalities necessary for working with the cloud-native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the Session Management Function (SMF), Policy Control Function (PCF), and so on. *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 11 (last accessed June 17, 2021).
13[C] propagate, toward the remote connected services layer of the remote endpoint, an IP address change notification message including the service connection identifier for the service connection and the new IP address of the apparatus.	Cisco's Ultra 5G propagates, towards the remote connected services layer of the remote endpoint, an IP address change notification message including the service connection identifier for the service connection and the new IP address of the apparatus. As one non-limiting example, Cisco's Ultra 5G through the SMF and IPAM handle IP address propagation (e.g., requests and releases) during session establishment and termination. The IPAM cache, client, and server manage address change notifications during this session establishment and termination process, including for new IP addresses.

	• **SMF Node-Manager Application** – The SMF Node-Manager application takes care of the UPF, ID resource, and IP address management. Therefore, the SMF Node-Manager application integrates IPAM Cache and IPAM client modules. The UPF Manager uses the IPAM Client module for address-range-reservation per UPF. • **SMF Service Application** – The SMF Service application provides PDU session services. During session establishment and termination, the IP addresses are requested and released back. The SMF Service application invokes the IPC to RMGR in Node Manager, which receives (free) the IP from the IPAM module. • **IPAM Server Application** – Based on the deployment model, the IPAM Server application can run as an independent microservice, as a part of the same cluster, or in a remote-cluster. For standalone deployments, the IPAM Servers are an integral part of the IPAM cache. *See id*. at 312.

	 *See id.*
CLAIM 14	
14[A] The apparatus of claim 13, wherein the apparatus is configured to detect the change of the apparatus from the	Cisco's Ultra 5G consists of an apparatus wherein the apparatus is configured to detect the change of the apparatus from the IP address to the new IP address. *See* 13[A], *supra*. As one non-limiting example, Cisco's Ultra 5G, through the IPAM Server and IPAM Client, detect the change of IP addresses as part of the modules' management functions.

IP address to the new IP address.	• **SMF Node-Manager Application** – The SMF Node-Manager application takes care of the UPF, ID resource, and IP address management. Therefore, the SMF Node-Manager application integrates IPAM Cache and IPAM client modules. The UPF Manager uses the IPAM Client module for address-range-reservation per UPF. • **SMF Service Application** – The SMF Service application provides PDU session services. During session establishment and termination, the IP addresses are requested and released back. The SMF Service application invokes the IPC to RMGR in Node Manager, which receives (free) the IP from the IPAM module. • **IPAM Server Application** – Based on the deployment model, the IPAM Server application can run as an independent microservice, as a part of the same cluster, or in a remote-cluster. For standalone deployments, the IPAM Servers are an integral part of the IPAM cache. *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 312 (last accessed June 17, 2021).

	 *See id.* The IPAM system includes the following sub-modules: • **IPAM Server** – The IPAM Server module manages the complete list of pools and address-space configuration. It splits the configured address-ranges into smaller address-ranges (statically and dynamically) and distributes it to the IPAM Cache modules. You can deploy the IPAM Server either as *See id.*

	• **IPAM Client** – The IPAM Client module handles the request and release of the individual IP addresses from the IPAM Cache for each IP managed end-device. Based on the use cases, the IPAM Client module caters the needs of specific network functions (such as SMF, PCF, and so on). *See id.* at 313.
CLAIM 15	
15[A] The apparatus of claim 13, wherein the connected services layer is configured to encrypt the IP address change notification message, using at least one encryption key associated with the service connection, prior to propagating the IP address change notification message.	Cisco's Ultra 5G consists of an apparatus wherein the connected services layer is configured to encrypt the IP address change notification message, using at least one encryption key associated with the service connection, prior to propagating the IP address change notification message. *See* 13[A], *supra*. Cisco's Ultra 5G header enrichment features append header information (e.g., "using at least one encryption key associated with the service connection, prior to propagating the IP address change notification message") to HTTP or WSP GET and POST request packets and HTTP response packets. With the X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, you can append headers to HTTP or WSP GET and POST request packets, and HTTP response packets for use by end applications. For example, mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on. *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02 – Configuration and Administration Guide, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF.pdf, at 181 (last accessed June 17, 2021).

<table>
<tr><td></td><td>

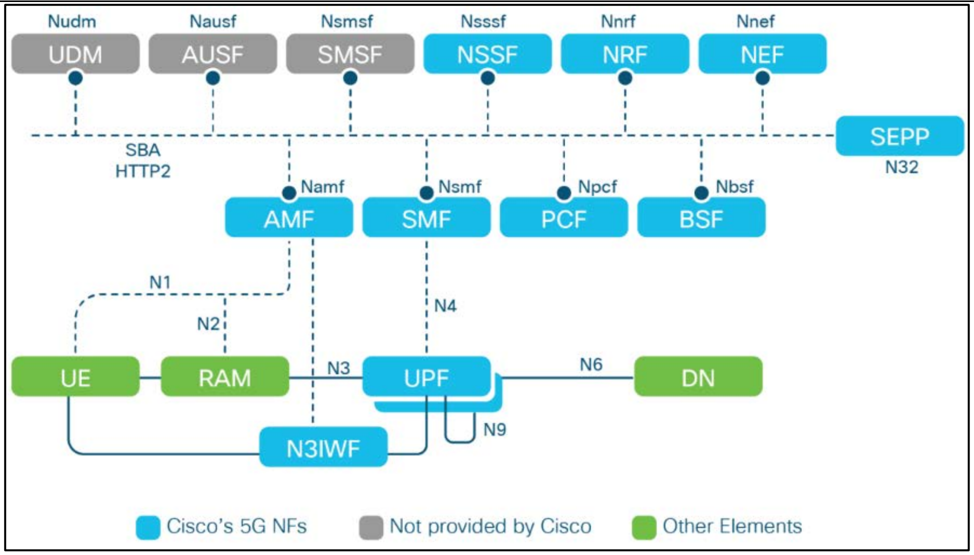
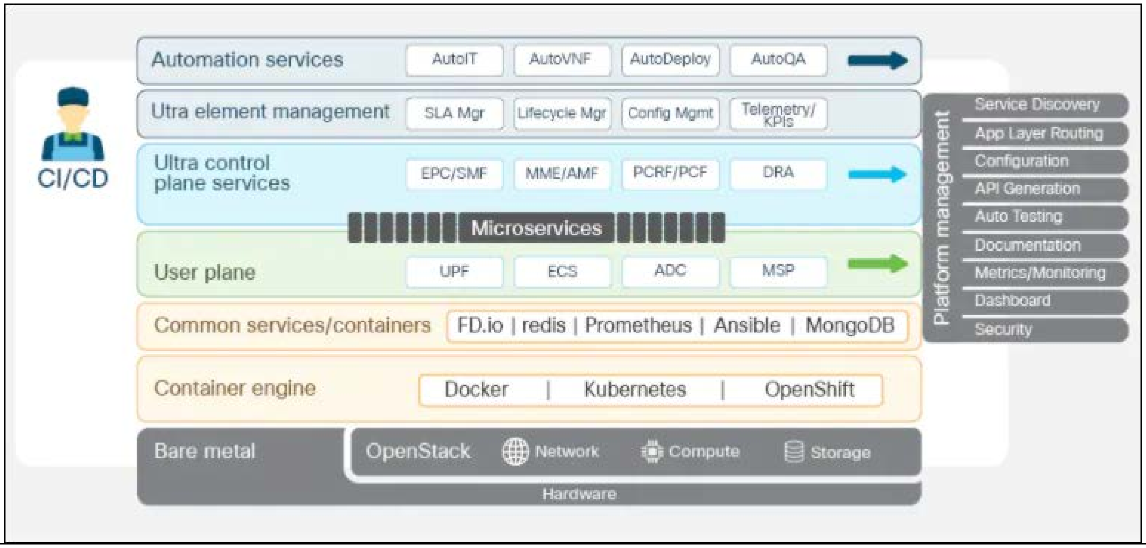
```
configure
   active-charging service acs_service_name
      xheader-format xheader_format_name
        insert xheader_field_name { string-constant xheader_field_value | variable
 { bearer { 3gpp { apn | charging-characteristics | charging-id | imei |

 imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id
| ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] | http { host | url } }
         end
```

See id. at 184-85.

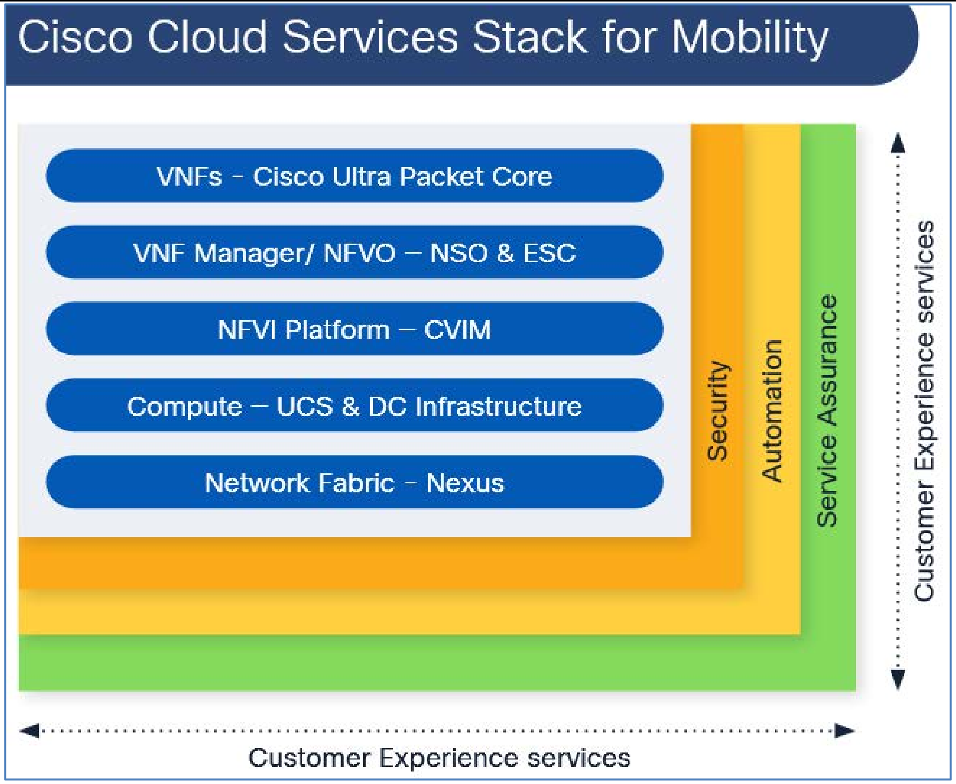
```
configure
   active-charging service acs_service_name
      charging-action charging_action_name
         xheader-insert xheader-format xheader_format_name [ encryption {
rc4md5 | aes-256-gcm-sha384 [ salt ] } [ encrypted ] key key ] [
first-request-only ] [ msg-type { response-only | request-and-response }
 ] [ -noconfirm ]
         end
```

See id. at 185.</td></tr>
<tr><td colspan="2">CLAIM 18</td></tr>
<tr><td>18[Pre.] A method, comprising:</td><td>To any extent the preamble is limiting, the Cisco Ultra Cloud Core and 5G Packet Core Solutions (“Cisco’s Ultra 5G”) comprise a method.

Cisco’s Ultra 5G provides cloud core and 5G packet core solutions (e.g., a “method”) which are based on the 3GPP 5G service-based architecture.</td></tr>
</table>

	 *See* 5G Network Architecture, CISCO, https://www.cisco.com/c/en/us/solutions/service-provider/5g-network-architecture.html, at 12 (last accessed June 17, 2021). 

	See Cisco's Cloud Core, CISCO, https://www.cisco.com/c/en/us/solutions/service-provider/mobile-internet/ultra-cloud-core-at-a-glance.html#~cisco's-cloud-core, at 2 (last accessed June 17, 2021).
18[A] running, by a processor, a connected services stack, the connected services stack comprising a connected services layer configured to operate below an application layer and above a transport layer, wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint, wherein the connected services layer is configured to support establishment of the service connection	Cisco's Ultra 5G practices a method comprising running, by a processor, a connected services stack, the connected services stack comprising a connected services layer configured to operate below an application layer and above a transport layer. **Cisco Cloud Services Stack for Mobility** enables **faster rollout of new services** by utilizing industry leading capabilities, mobile packet core software, and extensive Cisco experience and insights, leveraging: **Cisco's market-leading Ultra Packet Core**, deployed in the world's largest and most challenging mobile networks, and Cisco's **carrier-grade virtualization platform**, Cisco Virtual Infrastructure Manager (CVIM) **Cisco Solution Support** centralizes technical support across solution hardware and software, resolving complex issues 44% faster than product support[1] *See* Cisco Cloud Services Stack for Mobility, CISCO, https://www.cisco.com/c/dam/en_us/services/downloads/cisco-cloud-services-stack-mobility-at-a-glance.pdf, at 2 (last accessed June 17, 2021).

based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection, wherein the connected services layer is configured to:	 *See id*. at 2.

Cloud Core and Packet Core products

Cisco Ultra Cloud Core

We offer 5G standalone cloud native core for "any-cloud" deployment. Advanced features and automation speeds time to market, reduces risks, and saves money. Distributed CUPS enables multi-access edge computing.

Read data sheet ›

Cisco Ultra Packet Core

We offer an industry leading, converged, virtualized packet core for 5G, 4G, and Internet of Things (IoT). Among the most widely deployed packet cores, it is full featured with the scale and functionalities to meet demands and introduce services faster and more cost-effectively.

Read data sheet ›

Cloud Services Stack for Mobility

This is an industry leading virtualized packet core available for plug-and-play, pre-validated by Cisco Customer Experience (CX) and embedded with hardened security, automation, and assurance. You get all the benefits and none of the worry.

Read at-a-glance ›

See Cloud Core and Packet Core Portfolio, CISCO, https://www.cisco.com/c/en/us/products/wireless/packet-core/index.html#~features (last accessed June 17, 2021).

Cisco's Ultra 5G connected services stack offer various network functions (which are performed on at least one processor) such as Access and Mobility Management Functions (AMF), Policy Control Functions (PCF), Session Management Functions (SMF), Network Functions (NF) Repository Functions (NRF), Authentication Server Functions (AUSF), Network Exposure Functions (NEF), etc., which are a part of a connected services layer.

> Cisco's 5G SA portfolio is composed of all key mobile core network functions: Access and Mobility management Function (AMF), [[define]] SMF, UPF, PCF, Network Repository Function (NRF), Network Slice Selection Function (NSSF), Network Exposure Function (NEF), Binding Support Function (BSF), Non-3GPP Interworking Function (N3IWF), and Security Edge Protection Proxy (SEPP) (refer to Figure 11).

See 5G Network Architecture, CISCO, https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/pdfs/cisco-ultra-5g-packet-core-solution-wp-v1a.pdf, at 12 (last accessed June 17, 2021).

Cisco's Ultra 5G allows a NF to expose its service functionality through well-defined interfaces using the application layer protocol (e.g., HTTP/2) and transport layer protocol (e.g., TCP) to other authorized NFs. Thus, Cisco's Ultra 5G connected services stack is "configured to operate below an application layer and above a transport layer."

> The three-tiered architecture on which Cisco's CP NFs are designed full support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

See 5G Network Architecture, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/m_.pdf, at 5 (last accessed June 17, 2021).

Cisco's Ultra 5G further practices a method wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint.

For example, Cisco's Ultra 5G NF gets a list of NF instances that are registered with the NRF.

> **Nnrf_NFDiscovery**
>
> The Nnrf_NFDiscovery service allows a Network Function Instance to discover services offered by other Network Function Instances, by querying the local NRF.

See Nnrf_NFDiscovery, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/2020-02-0/b_SMF-API-Reference/b_test-SMF_chapter_010010.pdf, at 1 (last accessed June 17, 2021).

Further, Cisco's Ultra 5G practices a method wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection.

Cisco's Ultra 5G provides for NF consumers and NF producers to connect with each other by creating sessions to establish service connections (e.g., "the connected services layer is configured to support establishment of

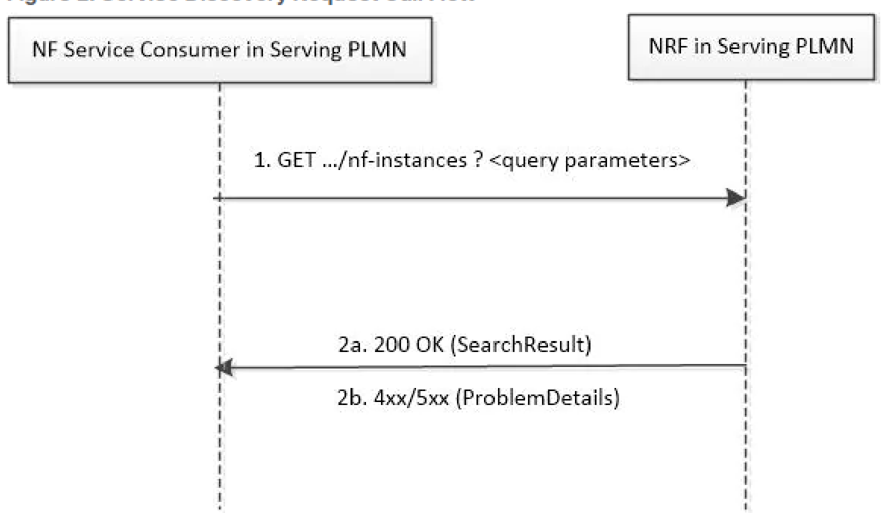
the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection”).

> The three-tiered architecture on which Cisco's CP NFs are designed full support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

See 5G Architecture, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/m_.pdf, at 5 (last accessed June 17, 2021).

Cisco’s Ultra 5G provides that an NF Consumer that needs to access the services of an NF producer can retrieve the ‘NFProfile’ of the NF producer by sending, e.g., an HTTP request to the NRF. The HTTP request contains the NF Instance ID of the consumer (e.g., “service name of the connected services layer”) and the NF instance ID of the Producer (e.g., “service name of the remote connected services layer”).

Figure 2. Service Discovery Request Call Flow



See Ultra Cloud Core 5G Session Management Function, Release 2020.02, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).

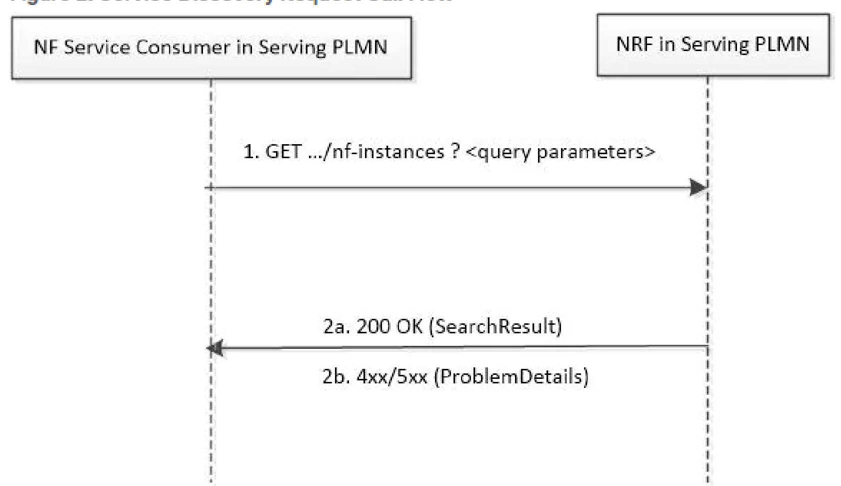
	NRF Discovery Support Based on the 3GPP-defined architecture model for 5G systems for data connectivity, SMF discovers the set of NF instances and their associate NF service instances. These instances, which are based on the NF profiles, are registered in the Network Repository Function (NRF) and meet the various input query parameters. *See id.* at 6. On success, "200 OK" is returned. The response body contains a validity period, during which the search result can be cached by the NF Service Consumer, and an array of NF profile object that satisfy the search filter criteria (for example, all NF Instances offering a certain NF Service name). *See id.* at 4. The NF 'serviceName' along with the 'version' act (e.g., "the service connection identifier") provide connection identification between the NF consumer and the NF producer. **6.5 NF Service Instance Reselection** If a formerly selected NF Service Instance becomes unavailable, the NF Service Consumer may select a different instance of a same NF Service, in the same NF Instance, if the NF Instance indicates in its NF Profile that it supports the capability to persist their resources in shared storage inside the NF Instance, and if the new NF Service Instance offers the same major service version. *See* 5G System Restoration Procedures, ETSI, https://www.etsi.org/deliver/etsi_ts/123500_123599/123527/15.03.00_60/ts_123527v150300p.pdf, at 19 (last accessed June 17, 2021). Further, Cisco's Ultra 5G practices said method wherein the connected services layer is configurable.

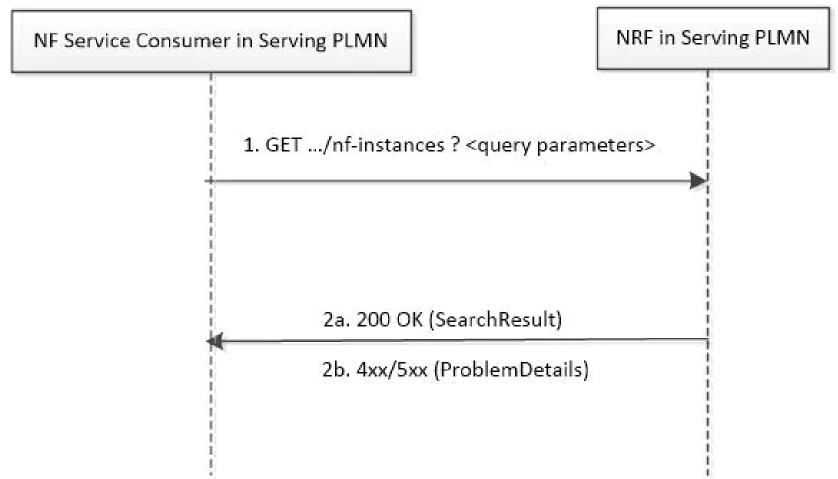
Features and benefits

Table 1. Ultra Cloud Core features and benefits

Feature	Benefit
Cisco intelligent service mesh	What it is: Intelligent service mesh routes traffic within the cluster to specific application instances. Result: Multiple variations and configurations of services can run concurrently. Result: New services and upgrades can be introduced with very low risk.
Common execution environment	What it is: Common components for logging, alarming, events, deployment, upgrades, configuration, and provisioning Result: Cisco 5G applications are configured the same, deployed the same, and share the same logging, alarming, telemetry components. Result: Onboarding additional Cisco applications is easy.
Cisco operations center	What it is: An agent can deploy applications using a YANG schema and expose NETCONF/RESTCONF interfaces to each product by integrating with Cisco Network Services Orchestrator. Result: Common API, command line interface (CLI), and GUI interface to each 5G application Result: All change management can be orchestrated.
Granular tracing	What it is: Integration with application dynamics and open tracing for traffic flow monitoring Result: A new level of visibility of traffic flows across network functions and between and within services
Release automation framework	What it is: This framework provides the ability to automate testing as part of the service deployment. Result: Testing becomes part of the service deployment workflow. Result: This automation reduces the time needed to certify new services, code, and new configurations, and reduces the time to market.

See Cisco Ultra Cloud Core Data Sheet, CISCO, https://www.cisco.com/c/en/us/products/collateral/wireless/packet-core/datasheet-c78-744630.html (last accessed June 17, 2021) (noting various Cisco Ultra 5G elements which are configurable).

	Thus, Cisco's Ultra 5G practices a method wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection.
18[B] send, toward a server, a service connection request message comprising the service name of the connected services layer and the service name of the remote connected services layer of the remote endpoint; and	Cisco's Ultra 5G practices a method comprising the step of sending, towards a server, a service connection request message comprising the service name of the connected services layer and the service name of the remote connected services layer of the remote endpoint. In Cisco's Ultra 5G, an NF Consumer can retrieve the NFProfile of an NF producer by sending a HTTP request to the NRF (e.g., "a server") containing an identifier of the consumer (e.g., "a service connection request message comprising the service name of the connected services layer") and an identifier of the NF Producer (e.g., "...and the service name of the remote connected services layer of the remote endpoint"). **Figure 2. Service Discovery Request Call Flow**  *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).
18[C] receive, from the server, a service	Cisco's Ultra 5G practices a method comprising the step of receiving, from the server, a service connection response message comprising the service name of the remote connected services layer of the remote endpoint,

connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection.	an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection. The NRF (e.g., "a server") receives the HTTP request and responds with an HTTP message containing an identifier that includes a Producer's NF instanceID, IP address, the service name, and the version (e.g., "a service connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection") for the connection. Figure 2. Service Discovery Request Call Flow  *See id.* at 3. **NFProfile** **Type**: object **Required**: - nfInstanceId - nfType - nfStatus

See Nnrf_NFDiscovery, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/2020-02-0/b_SMF-API-Reference/b_test-SMF_chapter_010010.pdf, at 10 (last accessed June 17, 2021).

ipv4Addresses:

Type: array

Items:

Reference: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'

minItems: 1

ipv6Addresses:

Type: array

See id. at 11.

nfServices:

Type: array

Items:

Reference: '#/components/schemas/NFService'

See id. at 12.

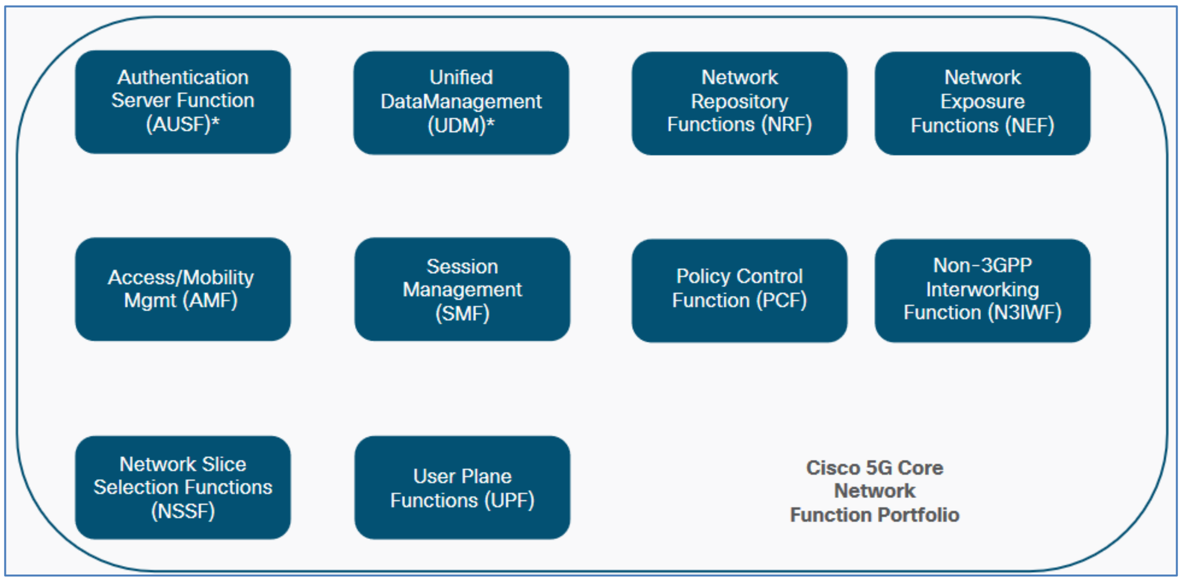
NFService

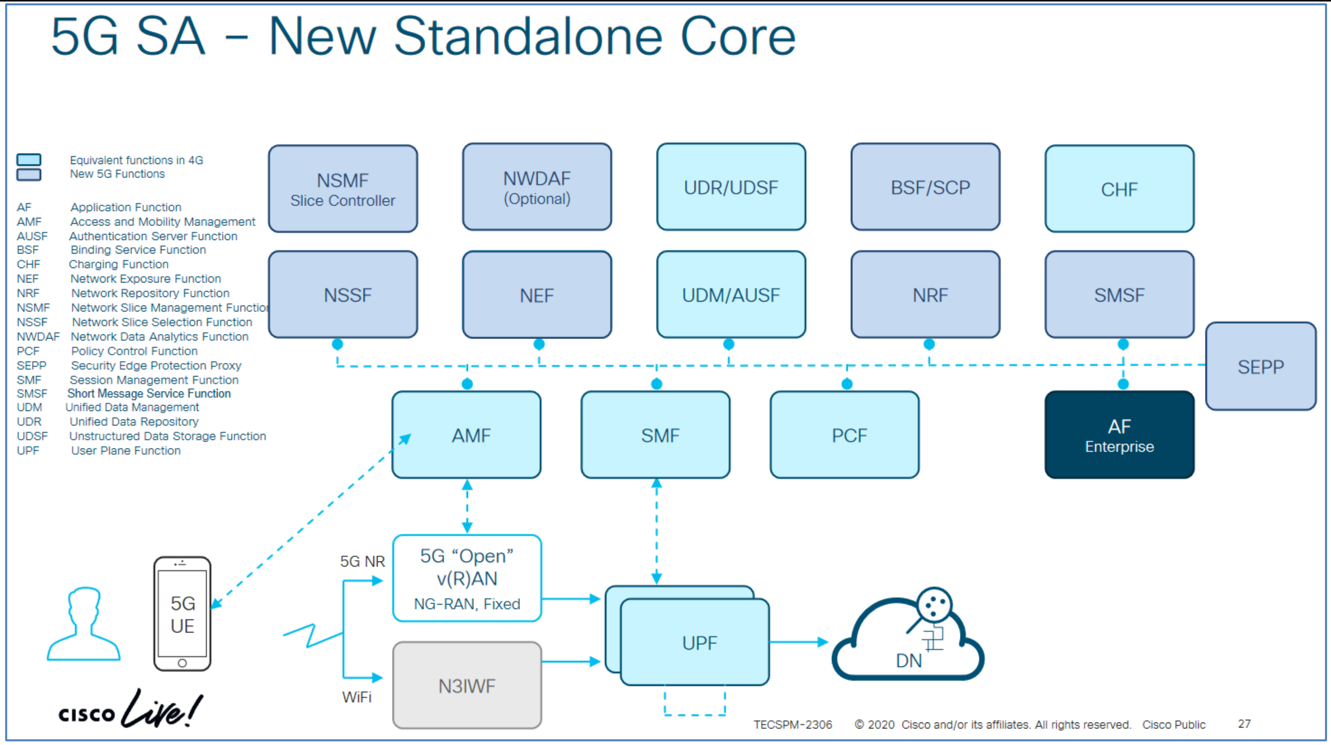
Type: object

Required:

- serviceInstanceId
- serviceName
- versions
- scheme
- nfServiceStatus

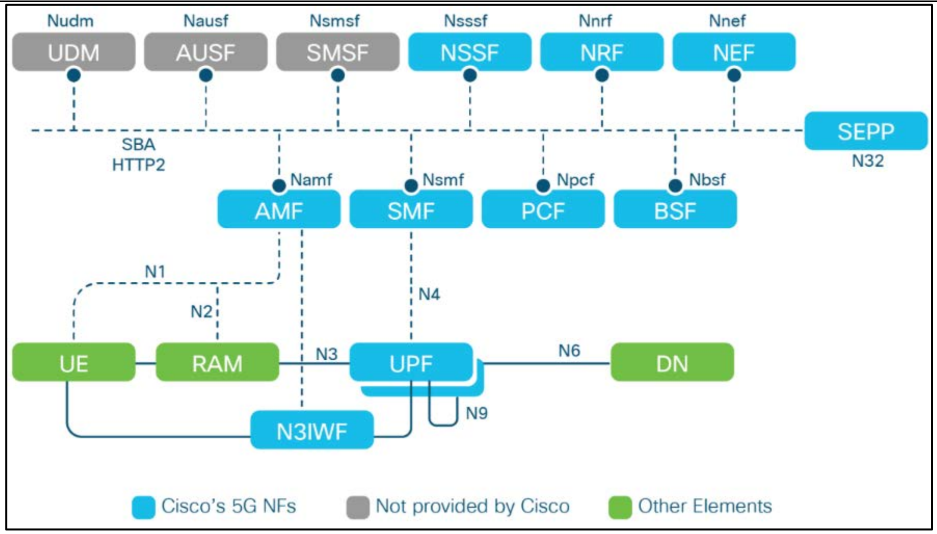
See id. at 13.

CLAIM 19	
19[Pre.] A non-transitory computer-readable storage medium storing instructions which, when executed by a computer, cause the computer to perform a method, the method comprising:	To any extent the preamble is limiting, the Cisco Ultra Cloud Core and 5G Packet Core Solutions ("Cisco's Ultra 5G") comprises a non-transitory computer-readable storage medium storing instructions which, when executed by a computer, cause the computer to perform a method. Cisco's Ultra 5G network function portfolio, as one non-limiting example, provides network functions like Access/Mobility Management (AMF) which support "registration management, access control and mobility management function for all 3GPP accesses as well as non-3GPP accesses such as WLAN" accomplished via a non-transitory computer-readable storage medium storing instructions which, when executed by, e.g., the AMF, cause the AMF to perform a method.  *See* Cisco Ultra 5G Packet Core Solution, CISCO, https://www.cisco.com/c/dam/en/us/products/collateral/routers/network-convergence-system-500-series-routers/white-paper-c11-740360.pdf, at 7-8 (last accessed June 17, 2021).

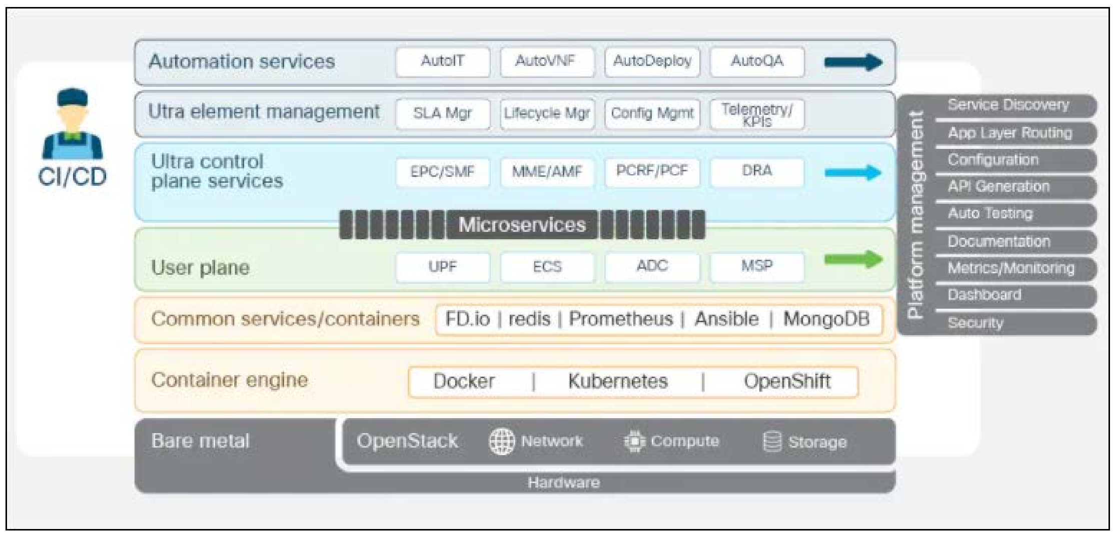


See 5G System – CISCO Proposal, CISCO, https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/R6BGArNQ/TECSPM-2306.pdf, at 27 (last accessed June 17, 2021).

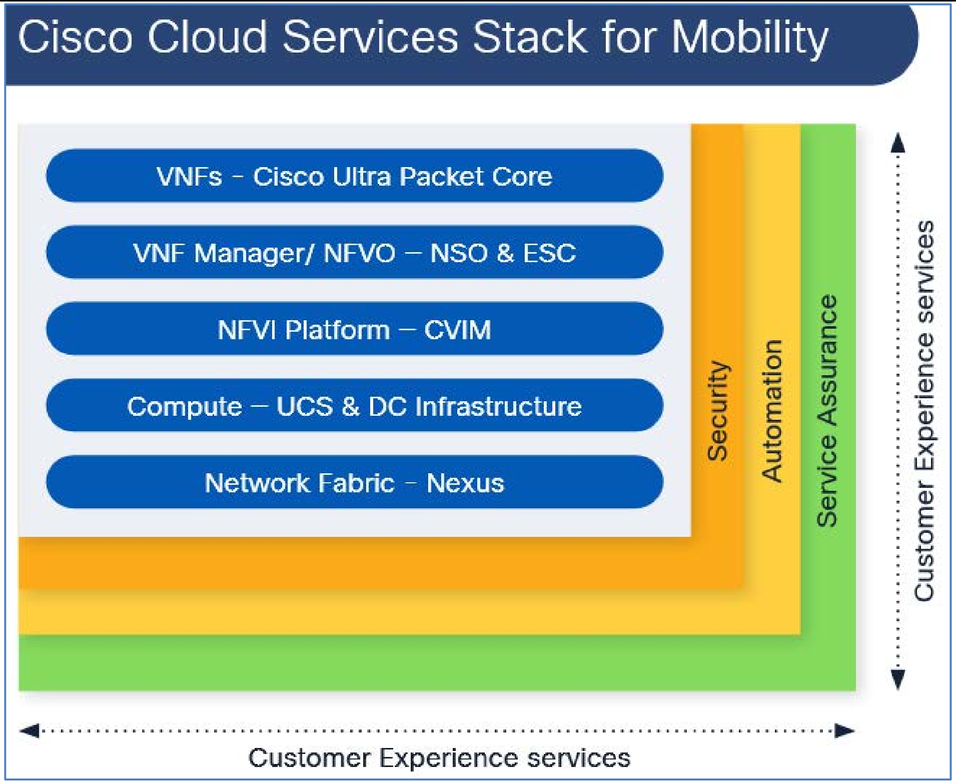
Cisco's Ultra 5G provides cloud core and 5G packet core solutions (e.g., a "method") which are based on the 3GPP 5G service-based architecture.



See 5G Network Architecture, CISCO, https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/pdfs/cisco-ultra-5g-packet-core-solution-wp-v1a.pdf, at 12 (last accessed June 17, 2021).



	See Cisco's Cloud Core, CISCO, https://www.cisco.com/c/en/us/solutions/service-provider/mobile-internet/ultra-cloud-core-at-a-glance.html#~cisco's-cloud-core, at 2 (last accessed June 17, 2021).
19[A] running a connected services stack, the connected services stack comprising a connected services layer configured to operate below an application layer and above a transport layer, wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint, wherein the connected services layer is configured to support establishment of the service connection based on a service	Cisco's Ultra 5G practices a method comprising running a connected services stack, the connected services stack comprising a connected services layer configured to operate below an application layer and above a transport layer. **Cisco Cloud Services Stack for Mobility** enables **faster rollout of new services** by utilizing industry leading capabilities, mobile packet core software, and extensive Cisco experience and insights, leveraging: **Cisco's market-leading Ultra Packet Core**, deployed in the world's largest and most challenging mobile networks, and Cisco's **carrier-grade virtualization platform**, Cisco Virtual Infrastructure Manager (CVIM) **Cisco Solution Support** centralizes technical support across solution hardware and software, resolving complex issues 44% faster than product support[1] *See* Cisco Cloud Services Stack for Mobility, CISCO, https://www.cisco.com/c/dam/en_us/services/downloads/cisco-cloud-services-stack-mobility-at-a-glance.pdf, at 2 (last accessed June 17, 2021).

name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection, wherein the connected services layer is configured to:	 *See* Cisco Cloud Services Stack for Mobility, CISCO, https://www.cisco.com/c/dam/en_us/services/downloads/cisco-cloud-services-stack-mobility-at-a-glance.pdf, at 2 (last accessed June 17, 2021).

Cloud Core and Packet Core products

Cisco Ultra Cloud Core

We offer 5G standalone cloud native core for "any-cloud" deployment. Advanced features and automation speeds time to market, reduces risks, and saves money. Distributed CUPS enables multi-access edge computing.

Read data sheet ›

Cisco Ultra Packet Core

We offer an industry leading, converged, virtualized packet core for 5G, 4G, and Internet of Things (IoT). Among the most widely deployed packet cores, it is full featured with the scale and functionalities to meet demands and introduce services faster and more cost-effectively.

Read data sheet ›

Cloud Services Stack for Mobility

This is an industry leading virtualized packet core available for plug-and-play, pre-validated by Cisco Customer Experience (CX) and embedded with hardened security, automation, and assurance. You get all the benefits and none of the worry.

Read at-a-glance ›

See Cloud Core and Packet Core Portfolio, CISCO, https://www.cisco.com/c/en/us/products/wireless/packet-core/index.html#~features (last accessed June 17, 2021).

Cisco's Ultra 5G connected services stack offer various network functions (which are performed on at least one processor) such as Access and Mobility Management Functions (AMF), Policy Control Functions (PCF), Session Management Functions (SMF), Network Functions (NF) Repository Functions (NRF), Authentication Server Functions (AUSF), Network Exposure Functions (NEF), etc., which are a part of a connected services layer.

> Cisco's 5G SA portfolio is composed of all key mobile core network functions: Access and Mobility management Function (AMF), [[define]] SMF, UPF, PCF, Network Repository Function (NRF), Network Slice Selection Function (NSSF), Network Exposure Function (NEF), Binding Support Function (BSF), Non-3GPP Interworking Function (N3IWF), and Security Edge Protection Proxy (SEPP) (refer to Figure 11).

See 5G Network Architecture, CISCO, https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/pdfs/cisco-ultra-5g-packet-core-solution-wp-v1a.pdf, at 12 (last accessed June 17, 2021).

Cisco's Ultra 5G allows a NF to expose its service functionality through well-defined interfaces using the application layer protocol (e.g., HTTP/2) and transport layer protocol (e.g., TCP) to other authorized NFs. Thus,

Cisco's Ultra 5G connected services stack is "configured to operate below an application layer and above a transport layer."

> The three-tiered architecture on which Cisco's CP NFs are designed full support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

See 5G Architecture, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/m_.pdf, at 5 (last accessed June 17, 2021).

Cisco's Ultra 5G further practices a method wherein the connected services layer is configured to support establishment of a service connection between the connected services layer and a remote connected services layer of a remote endpoint.

For example, Cisco's Ultra 5G NF gets a list of NF instances that are registered with the NRF.

> **Nnrf_NFDiscovery**
>
> The Nnrf_NFDiscovery service allows a Network Function Instance to discover services offered by other Network Function Instances, by querying the local NRF.

See Nnrf_NFDiscovery, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/2020-02-0/b_SMF-API-Reference/b_test-SMF_chapter_010010.pdf, at 1 (last accessed June 17, 2021).

Further, Cisco's Ultra 5G practices a method wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection.

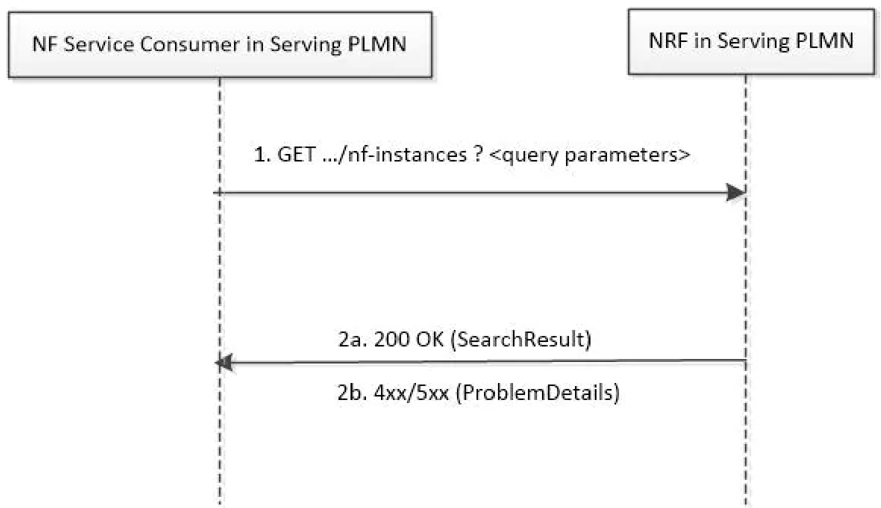
Cisco's Ultra 5G provides for NF consumers and NF producers to connect with each other by creating sessions to establish service connections (e.g., "the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection").

> The three-tiered architecture on which Cisco's CP NFs are designed full support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

See 5G Architecture, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/m_.pdf, at 5 (last accessed June 17, 2021).

Cisco's Ultra 5G provides that an NF Consumer that needs to access the services of an NF producer can retrieve the 'NFProfile' of the NF producer by sending, e.g., an HTTP request to the NRF. The HTTP request contains the NF Instance ID of the consumer (e.g., "service name of the connected services layer") and the NF instance ID of the Producer (e.g., "service name of the remote connected services layer").

Figure 2. Service Discovery Request Call Flow



See Ultra Cloud Core 5G Session Management Function, Release 2020.02, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).

	NRF Discovery Support Based on the 3GPP-defined architecture model for 5G systems for data connectivity, SMF discovers the set of NF instances and their associate NF service instances. These instances, which are based on the NF profiles, are registered in the Network Repository Function (NRF) and meet the various input query parameters. *See id*. at 6. On success, "200 OK" is returned. The response body contains a validity period, during which the search result can be cached by the NF Service Consumer, and an array of NF profile object that satisfy the search filter criteria (for example, all NF Instances offering a certain NF Service name). *See id*. at 4. The NF 'serviceName' along with the 'version' act (e.g., "the service connection identifier") provide connection identification between the NF consumer and the NF producer. 6.5 NF Service Instance Reselection If a formerly selected NF Service Instance becomes unavailable, the NF Service Consumer may select a different instance of a same NF Service, in the same NF Instance, if the NF Instance indicates in its NF Profile that it supports the capability to persist their resources in shared storage inside the NF Instance, and if the new NF Service Instance offers the same major service version. *See* 5G System Restoration Procedures, ETSI, https://www.etsi.org/deliver/etsi_ts/123500_123599/123527/15.03.00_60/ts_123527v150300p.pdf, at 19 (last accessed June 17, 2021). Further, Cisco's Ultra 5G practices said method wherein the connected services layer is configurable.

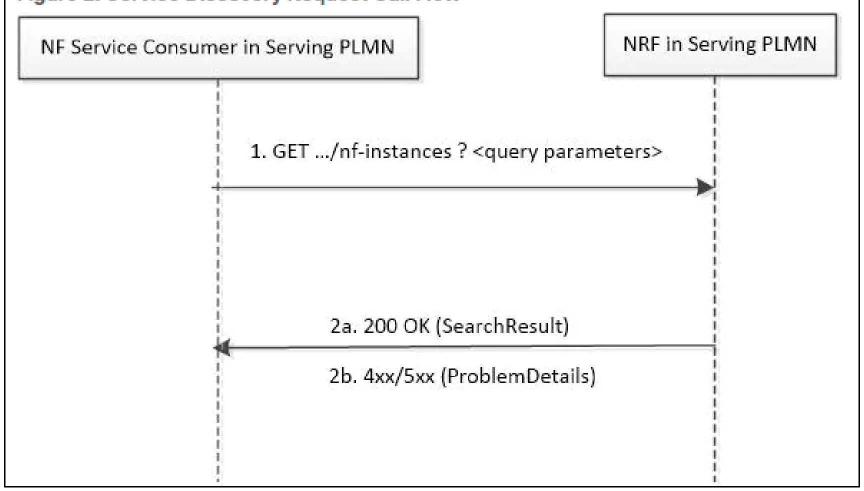
	Features and benefits **Table 1. Ultra Cloud Core features and benefits** (see table below)

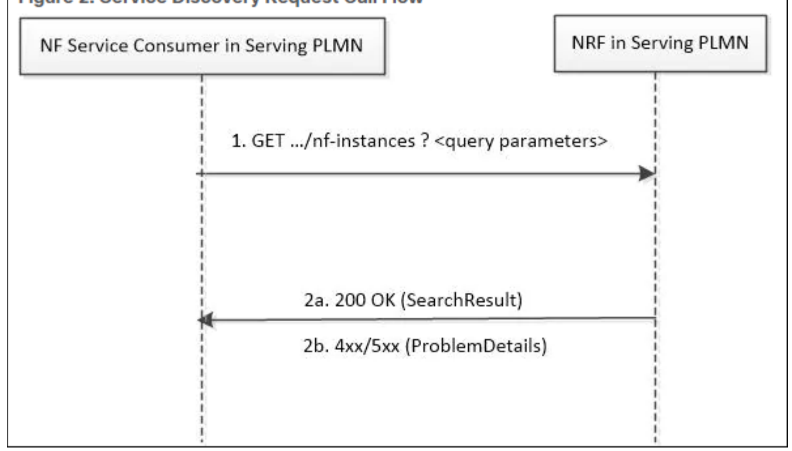
Features and benefits

Table 1. **Ultra Cloud Core features and benefits**

Feature	Benefit
Cisco intelligent service mesh	What it is: Intelligent service mesh routes traffic within the cluster to specific application instances. Result: Multiple variations and configurations of services can run concurrently. Result: New services and upgrades can be introduced with very low risk.
Common execution environment	What it is: Common components for logging, alarming, events, deployment, upgrades, configuration, and provisioning Result: Cisco 5G applications are configured the same, deployed the same, and share the same logging, alarming, telemetry components. Result: Onboarding additional Cisco applications is easy.
Cisco operations center	What it is: An agent can deploy applications using a YANG schema and expose NETCONF/RESTCONF interfaces to each product by integrating with Cisco Network Services Orchestrator. Result: Common API, command line interface (CLI), and GUI interface to each 5G application Result: All change management can be orchestrated.
Granular tracing	What it is: Integration with application dynamics and open tracing for traffic flow monitoring Result: A new level of visibility of traffic flows across network functions and between and within services
Release automation framework	What it is: This framework provides the ability to automate testing as part of the service deployment. Result: Testing becomes part of the service deployment workflow. Result: This automation reduces the time needed to certify new services, code, and new configurations, and reduces the time to market.

See Cisco Ultra Cloud Core Data Sheet, CISCO, https://www.cisco.com/c/en/us/products/collateral/wireless/packet-core/datasheet-c78-744630.html (last accessed June 17, 2021) (noting various Cisco Ultra 5G elements which are configurable).

	Thus, Cisco's Ultra 5G practices a method wherein the connected services layer is configured to support establishment of the service connection based on a service name of the connected services layer, a service name of the remote connected services layer, and a service connection identifier for the service connection.
19[B] send, toward a server, a service connection request message comprising the service name of the connected services layer and the service name of the remote connected services layer of the remote endpoint; and	Cisco's Ultra 5G practices a method comprising the step of sending, towards a server, a service connection request message comprising the service name of the connected services layer and the service name of the remote connected services layer of the remote endpoint. In Cisco's Ultra 5G, an NF Consumer can retrieve the NFProfile of an NF producer by sending a HTTP request to the NRF (e.g., "a server") containing an identifier of the consumer (e.g., "a service connection request message comprising the service name of the connected services layer") and an identifier of the NF Producer (e.g., "...and the service name of the remote connected services layer of the remote endpoint"). Figure 2. Service Discovery Request Call Flow  *See* Ultra Cloud Core 5G Session Management Function, Release 2020.02, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/b_SMF/b_SMF_chapter_011100.html, at 3 (last accessed June 17, 2021).
19[C] receive, from the server, a service	Cisco's Ultra 5G practices a method comprising the step of receiving, from the server, a service connection response message comprising the service name of the remote connected services layer of the remote endpoint,

connection response message comprising the service name of the remote connected remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection.	an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection. The NRF (e.g., “a server”) receives the HTTP request and responds with an HTTP message containing an identifier that includes a Producer’s NF instanceID, IP address, the service name, and the version (e.g., “a service connection response message comprising the service name of the remote connected services layer of the remote endpoint, an Internet Protocol (IP) address of the remote endpoint, and the service connection identifier for the service connection”) for the connection.  Figure 2. Service Discovery Request Call Flow *See id.* **NFProfile** **Type**: object **Required**: - nfInstanceId - nfType - nfStatus

	See Nnrf_NFDiscovery, CISCO, https://www.cisco.com/c/en/us/td/docs/wireless/ucc/smf/2020-02-0/b_SMF-API-Reference/b_test-SMF_chapter_010010.pdf, at 10 (last accessed June 17, 2021). **ipv4Addresses**: **Type**: array **Items**: **Reference**: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr' **minItems**: 1 **ipv6Addresses**: **Type**: array *See id*. at 11. **nfServices**: **Type**: array **Items**: **Reference**: '#/components/schemas/NFService' *See id*. at 12. NFService **Type**: object **Required**: - serviceInstanceId - serviceName - versions - scheme - nfServiceStatus *See id*. at 13.